101-04399/

LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00244 8810

THE LEGISLATIVE ASSEMBLY OF
BRITISH COLUMBIA

Special Committee on Information Privacy in the Private Sector

Report

2001

LEGISLATIVE LIBRARY
VICTORIA B.C. MAR 3 0 2001

National Library of Canada Cataloguing in Publication Data

British Columbia. Legislative Assembly. Special Committee on Information Privacy in the Private Sector.
Special Committee on Information Privacy in the Private Sector report

Report for the 4th Session, 36th Parliament. Cf. Covering letter.
Submitted to Legislative Assembly of British Columbia. Cf. Covering letter.

ISBN 0-7726-4527-2

1. Privacy, Right of - British Columbia. 2. Business records – Law and legislation – British Columbia. 3. Electronic records – British Columbia. 4. Electronic commerce – Law and legislation – British Columbia. I. Title.

KEB505.62S63 2001 342.71'0858 C2001-960099-2
KF5753.I5S63 2001

OFFICE OF THE CLERK OF COMMITTEES

Location:
Room 224, Parliament Buildings
Victoria, British Columbia
V8V 1X4

Telephone:	**(250) 356-2933**
Toll free at:	**1-877-428-8337**
Fax:	**(250) 356-8172**
Email:	**ClerkComm@leg.bc.ca**

Internet Homepage:
This report and others are available at our Internet Homepage which also contains further information about this and other Select Standing and Special Committees: **http://www.legis.gov.bc.ca/cmt**

March 20, 2001

To the Honourable,
The Legislative Assembly of
the Province of British Columbia
Victoria, British Columbia

Honourable Members:

We have the honour to present the *Report* of the Special Committee on Information Privacy in the Private Sector for the Fourth Session of the Thirty-Sixth Parliament.

Respectfully submitted on behalf of the Committee.

Mr. Rick Kasper, MLA
Chair

Mr. John Weisbeck, MLA
Deputy Chair

TABLE OF CONTENTS

TERMS OF REFERENCE 1

COMMITTEE MEMBERSHIP 3

COMMITTEE PROCESS 5

EXECUTIVE SUMMARY 7

RECOMMENDATIONS 9

PART 1 – THE CONTEXT OF INFORMATION PRIVACY 13

- The Information Economy 15
- Information Technologies 16
- Information Practices in BC's Private Sector 20
- British Columbians' Views on Information Privacy 23
- Employee Information 25
- Health Information 26
- Information Privacy Rights 31
- Fair Information Principles 33
  - Accountability 34
  - Identification of Purposes 34
  - Consent 35
  - Limiting Collection 36
  - Limited Use, Disclosure and Retention 36
  - Accuracy 37
  - Safeguards (Security) 37
  - Openness 37
  - Individual Access 37
  - Mechanisms for Challenging Compliance 38

PART 2 – INFORMATION PRIVACY RULES FOR BRITISH COLUMBIA'S PRIVATE SECTOR 39

- Legislation 39
- Self-regulation 41
- Harmonization 42
- CSA Model Code for the Protection of Personal Information 43
- Sectoral Codes of Practice 44
- The Right to Information Privacy 45
- Justification of Purposes 45
- Intrusive Processes 46

Scope of Application 47

Health information 48

Electronic Transactions 51

Exceptions 52

Publicly available information 52

Archival purposes 53

Credit Reporting 53

Accountability 54

Fees 54

Oversight 55

Educational initiatives 56

PART 3 – BILL 32 — ELECTRONIC TRANSACTIONS ACT 59

APPENDIX I – IPSOS REID - DETAILED FINDINGS: QUANTITATIVE STUDY 63

APPENDIX II – SURVEY 79

APPENDIX III – WITNESS LIST 85

APPENDIX IV – REFERENCES 87

TERMS OF REFERENCE

On July 14, 1999 during the 3rd Session of the 36th Parliament, The Honourable Joy MacPhail moved the following motion to appoint the Special Committee on Information Privacy in the Private Sector:

> *a Special Committee be appointed to examine, inquire into and make recommendations with respect to:*
>
> 1 *the protection of personal information in private sector transactions and*
>
> 2. *the impact of electronic documents on privacy and freedom of information for British Columbians; and without limiting the generality of the foregoing to consider reports referred to the Committee by the Minister of Advanced Education, Training and Technology.*
>
> *The Special Committee so appointed shall have the powers of a Select Standing Committee and is also empowered:*
>
> (a) *to appoint of their number, one or more subcommittees and to refer to such subcommittees any of the matters referred to the Committee;*
>
> (b) *to sit during a period in which the House is adjourned, during the recess after prorogation until the next following Session and during any sitting of the House;*
>
> (c) *to adjourn from place to place as may be convenient;*
>
> (d) *to retain such personnel as required to assist the Committee;*
>
> *and shall report to the House as soon as possible, or following any adjournment, or at the next following Session, as the case may be; to deposit the original of its reports with the Clerk of the Legislative Assembly during a period of adjournment and upon resumption of the sittings of the House, the Chair shall present all reports to the Legislative Assembly.*

On April 3, 2000, the Honourable Dale Lovick moved a motion to re-appoint the Special Committee on Information Privacy in the Private Sector for the 4th Session of the 36th Parliament with the same Terms of Reference.

COMMITTEE MEMBERSHIP

MEMBERS

Rick Kasper, MLA	Chair	Malahat-Juan de Fuca
John Weisbeck, MLA	Deputy Chair	Okanagan East
George Abbott, MLA		Shuswap
Pietro Calendino, MLA		Burnaby North
Glen Clark, MLA		Vancouver-Kingsway
Hon. Gerard Janssen, MLA *(to November 2000)*		Alberni
Steve Orcherton, MLA		Victoria-Hillside
Geoff Plant, MLA		Richmond-Steveston
Jan Pullinger, MLA *(from November 2000)*		Cowichan-Ladysmith
Erda Walsh, MLA		Kootenay
Katherine Whittred, MLA		North Vancouver-Lonsdale

CLERK TO THE COMMITTEE

Craig James
Clerk of Committees and Clerk Assistant

COMMITTEE RESEARCHER

Wynne MacAlpine
Committee Research Analyst

COMMITTEE PROCESS

The Legislative Assembly of British Columbia appointed the Special Committee on Information Privacy in the Private Sector on July 14, 1999, during the 3rd session of the 36th Parliament. The Committee was mandated to examine:

> *1. the protection of personal information in private sector transactions and*
>
> *2. the impact of electronic documents on privacy and freedom of information for British Columbians.*[1]

The Committee was struck as a result of the findings of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act.* In its June 1999 report to the Legislative Assembly, the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* reported that

> *British Columbia is already late in considering the issue of extending freedom of information and protection of privacy legislation to the private sector, not least because the federal government is planning to pass legislation in this area that will impact the provincial private sectors. The federal Bill C-54, Personal Information Protection and Electronic Documents Act* [passed as Bill C-6], *would extend its private sector information and privacy regulations to the provincial private sectors three years after its enactment.*[2]

That Committee also acknowledged that a number of developments have raised the profile of private sector information practices, particularly the movement towards private-public partnerships; the emergence of private sector applications for new information and surveillance technologies, such as smart cards, keystroke-monitoring, and biometric identification systems; and federal and provincial policies to network health information systems. The Special Committee to Review the *Freedom of Information and Protection of Privacy Act* expressed "support for government initiatives to manage any threats to privacy that arise out of new information technologies" and reported that "the development of information and privacy legislation for the provincial private sector is an urgent issue that requires further examination by government."[3]

In November 1999, the Special Committee on Information Privacy in the Private Sector began its inquiry with briefings on the meaning of privacy in the private sector context and the status of privacy regulation other jurisdictions by BC's Information and Privacy Commissioner, David Loukidelis, and representatives of the Information, Science and Technology Agency - the government agency responsible for privacy, information technologies and e-commerce in British Columbia. Again in June and July 2000, representatives of the Corporate Privacy and Information Access Branch of the Information, Science and Technology Agency briefed the Committee on select topics relating to information privacy in the private sector. In September 2000, the Committee invited witnesses Dr. Jochen Moehr from the School of Health Information Science at the University of Victoria, Dr. Richard Rosenberg from the Department of Computer Science at the University of British Columbia, and the Information and Privacy Commissioner to speak on their areas of expertise: health information systems, information technologies and privacy.

As part of the research process, as well, some individual members of the Committee attended conferences on topics such as the effect of the *Personal Information Protection and Electronic Documents Act* on private sector information management practices, the influence of the Internet on society, and the role that privacy-enhancing technologies can play in protecting information privacy in private sector transactions.

Members of the Committee on Information Privacy in the Private Sector committed to consulting with private sector enterprises and interested individuals and organizations on information privacy in the private sector. Through consultations with British Columbians, the Committee sought to gather opinions on a number of questions relating to information privacy and the BC private sector, such as:

> *What are the responsibilities of private sector enterprises in the use of individual's personal information?*
>
> *How does new information technology, such as that used in e-commerce and data mining, impact the private sector use of personal information?*
>
> *What form of regulation is most appropriate: self-regulation through organizational or sectoral codes, or legislation?*
>
> *What type of oversight mechanism is necessary to enforce the protection of personal information collected, used and disclosed by private sector organizations?*

To assist the Committee in beginning its public consultations, the Ministry of Advanced Education, Training and Technology published "A Discussion Paper: Protecting Personal Privacy in the Private Sector" in October 1999. The discussion paper outlined the significance of information privacy for BC's private sector and invited the public to participate in the Committee's consultations.

The Committee also undertook several initiatives to invite public participation. In December 1999 and January 2000, the Committee published advertisements requesting the public to send in their written submissions. Those advertisements also invited individuals and organizations to participate in the Committees' public hearings, which were held in Vancouver, Richmond, and Victoria in late January 2000. The Committee also sent an Invitation to Participate to over one hundred representative private sector businesses, business and consumer associations, and other non-governmental organizations in May 2000.

Finally, as part of its investigation, the Special Committee commissioned the Ipsos-Reid Corporation to conduct opinion research among British Columbians, both private citizens and business representatives, to understand their views on this issue. Ipsos-Reid conducted a multi-phase study consisting of depth interviews with members of the business community, and focus groups and a telephone survey with the general population. The results of the survey are contained in Appendix 1 of this report.

Members of the Committee would like to express their appreciation to the individuals and agencies that assisted the Committee with its work: those witnesses that appeared before the Committee and those who provided written submissions; David Loukidelis, BC's Information and Privacy Commissioner; Chris Norman, Director of the Corporate Privacy and Information Access Branch of the Information, Science and Technology Agency; Maggie Estok and Cathy Forrest of Ipsos-Reid; the Office of the Clerk of Committees; and Hansard Services.

EXECUTIVE SUMMARY

The Special Committee on Information Privacy in the Private Sector began its review by looking at the broader context of information privacy: the emergence of information privacy and the private sector as a public policy issue and the development of the universal fair information principles that have been adopted around the world as a means of protecting the privacy of personal information. Information privacy achieved official recognition in many Western nations in the 1980s as legislators recognized that computerized records greatly increased potential threats to individuals' privacy. Many countries adopted information privacy legislation to regulate the use of personal information in public sector activities at that time. The first international instruments for information privacy also emerged.

The Committee also reviewed the developments that have most recently given rise to widespread concern about the privacy of personal information held in all kinds of private sector settings. In the globalized economy, personal information is a valuable resource for business, one that is necessary to build relationships with customers now that transactions are more often than not attenuated by the sheer size of the marketplace, or by electronic media. Using information technologies, businesses have in recent years augmented their capacity to collect, process and transfer personal information, sometimes to the detriment of individuals' privacy. Information technologies and the globalized economy have raised the profile of information privacy and in turn brought attention to the conventional ways that personal information is collected, used and disclosed for a wide variety of private sector activities, including administration, market research, personnel management, the provision of health care and health research.

Committee members also considered the views of private sector businesses and organizations, interested individuals and privacy advocates. The Committee heard that British Columbians are in fact concerned about information privacy and support its regulation. Businesses want privacy rules to help them build trust with consumers and clients, and they want to operate in a regulatory environment that is consistent for all businesses in all jurisdictions. Consumers want their personal information to be used properly and only by those who need to use it. The concerns of some individuals and organizations incorporate the wide implications of private sector information use for both individuals and society as a whole, especially its impact on the human and civil rights that enrich our society.

The Committee learned that concerns like these are common to individuals, businesses, advocates and legislators throughout the information society. Western nations have responded by developing a set of fair information principles that can be applied to private sector activities in order to maintain both information privacy rights and businesses' ability to use personal information for legitimate purposes. In Canada, the *Personal Information Protection and Electronic Documents Act* has given legal effect to the fair information principles for the federally regulated private sector. In January 2004, the federal Act will apply to the provincially regulated private sector in provinces that have not enacted similar legislation.

Finally, pursuant to its Terms of Reference, the Committee examined the status of electronic transactions in public and private sector activities. The Committee noted that to enable Canadian businesses to take advantage of their potential e-commerce market share, governments have been called upon to limit impediments to the growth of electronic commerce by establishing a harmonized regulatory framework throughout Canada to support e-business. That framework includes not only measures to protect the privacy of personal information, but also to recognize the legality of electronic transactions and to support the security of electronic transmissions.

RECOMMENDATIONS

The Committee's recommendations reflect its four primary findings.

First, any policy adopted by British Columbia on the matter of information privacy in the private sector must consider the implications of the federal *Personal Information Protection and Electronic Documents Act* for this province. That legislation states that in January 2004, it will apply to British Columbia and any other province that has not passed privacy legislation for the provincial private sector that is deemed "substantially similar" by the federal government.[5] It is thought that the criteria for similarity include the "fair information principles" of consent and limited collection, use and disclosure, and an oversight mechanism empowered to regulate private sector compliance with the legislation.[6] The Committee would like to stress that its recommendations must be viewed in the context of the parameters established by the *Personal Information Protection and Electronic Documents Act.*

Secondly, the Committee found that British Columbians, both businesses and consumers, solidly support legislation to regulate information privacy in the private sector. British Columbia businesses have great potential to thrive as part of the global economy, and businesses say that privacy regulations that will foster consumer confidence can help them to fulfil their potential. Effective and efficient privacy legislation will provide clear rules for both consumers and business, satisfy consumers that all private sector organizations are respecting their personal information, and create a "level playing field" for information usage among and within industry sectors. Individuals are also extremely supportive of information privacy legislation. The Committee found that 92 percent of British Columbians agree that BC needs an information privacy law for the private sector.

Thirdly, British Columbians insist that any proposed privacy law must balance the private sector's needs to use personal information with consumers' rights to information privacy. Businesses and individuals were also in agreement that the fair information principles, such as those expressed by the Canadian Standards Association Model Code for the Protection of Personal Information, have successfully balanced the two. The ten interrelated fair information principles uphold the individual's ability to control the collection, use and disclosure of his or her personal information and provide businesses with reasonable, flexible guidelines on appropriate information practices.

The fourth understanding that shapes the Committee's recommendations is the consensus among individuals, businesses, privacy advocates and legislators that private sector privacy laws must be harmonized among all jurisdictions in which private sector organizations do business; in the information economy that means among all of the Canadian provinces and territories, and even with international trading partners.

RECOMMENDATION 1 — INFORMATION PRIVACY LEGISLATION FOR BRITISH COLUMBIA'S PRIVATE SECTOR

The Committee recommends that the government of British Columbia enact legislation to protect the information privacy of personal information held in the private sector, and that the proposed legislation achieve a fair and workable balance between information privacy and the use of personal information for legitimate private sector purposes.

RECOMMENDATION 2 — HARMONIZATION

The Committee recommends that proposed legislation harmonize with other Canadian and international jurisdictions, particularly the federal *Personal Information Protection and Electronic Documents Act*, by establishing a legal framework based on the internationally-recognized fair information principles such as those expressed by the Canadian Standards Association Model Code for the Protection of Personal Information: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

RECOMMENDATION 3 — SECTORAL CODES OF PRACTICE

The Committee recommends that private sector businesses and organizations be encouraged to develop and adopt privacy codes to assist them in implementing and complying with the fair information principles, and in educating their consumers, clients and employees.

RECOMMENDATION 4 — APPLICATION TO THE PRIVATE SECTOR

The Committee recommends that proposed legislation to protect the information privacy of British Columbians apply to all of the provincially-regulated private sector - all businesses and organizations not falling under the jurisdiction of the BC *Freedom of Information and Protection of Privacy Act* - while recognizing the need for a fair and workable balance between information privacy and the use of personal information for legitimate private sector purposes, as noted in recommendation 1.

RECOMMENDATION 5 — APPLICATION TO PRIVATE SECTOR ACTIVITIES

The Committee recommends that proposed legislation apply uniformly and consistently to all activities undertaken in the provincial private sector - not limited to "commercial activity" - subject to the exceptions discussed in recommendation 6.

RECOMMENDATION 6 — EXCEPTIONS

The Committee recommends that government consider and consult with relevant parties on any specific and limited exceptions to proposed legislation, including:

a) "publicly available" information, in order to balance the need for this particular class of personal information to be used for marketing and other purposes, but to protect individuals from obtaining it for purposes harmful to the data subject's well-being, health or safety.

b) personal information for activities relating to journalism, art and literature; law enforcement; emergencies concerning the life, health, security or best interests of an individual; scholarly study; and archival purposes.

c) personal information when required for collecting a debt; complying with a court order; or participating in legal proceedings.

RECOMMENDATION 7 — FEES

The Committee recommends that private sector organizations, interest groups and the public be consulted on the appropriateness of fees for administrative services when responding to requests for access to personal information held by private sector organizations. If fees are deemed appropriate to charge, proposed legislation should require that an estimate be required in advance of proceeding with a response to a request. Proposed legislation might also indicate that requests should be fulfilled in a timely manner.

RECOMMENDATION 8 — OVERSIGHT

The Committee recommends that proposed legislation provide for an oversight mechanism.

PART 1 – THE CONTEXT OF INFORMATION PRIVACY

On January 1, 2001, the federal *Personal Information Protection and Electronic Documents Act* came into effect, establishing "a right to the protection of personal information collected, used or disclosed in the course of commercial activities."[7] Until 2004, the Act will apply only to the federally regulated private sector, which includes telecommunications, broadcasting, banking, interprovincial transportation, and interprovincial and international trade. In January 2004, however, it will also extend to commercial activities undertaken in the provincially regulated private sector unless the Province has passed legislation that the federal government deems "substantially similar" to the federal Act.[8]

In establishing a right to the protection of personal information, the *Personal Information Protection and Electronic Documents Act* has given legal effect to ten "fair information principles": accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. These principles require private sector organizations to fulfil a number of responsibilities with respect to the personal information they collect, use and disclose in the course of their commercial activities. Under most circumstances, they must obtain an individual's consent for the collection, use or disclosure of his or her personal information. They must provide an individual with access to his or her information and allow an individual to make corrections to that information when necessary. They must also maintain the security of the personal information they hold.

The Legislation also empowers the federal Privacy Commissioner to oversee compliance with the provisions of the Act. The Privacy Commissioner can receive, investigate and mediate complaints about organizations that are not complying with the legislation. In the case of an investigation, the Commissioner must provide the parties to the complaint with a report of his or her findings and recommendations. While the Commissioner cannot issue compliance orders, parties to a dispute can request that the Federal Court review the report, and the Federal Court can order compliance and/or award damages. The Privacy Commissioner is empowered to publish the results of investigations, to initiate a complaint against an organization, and to audit the information management practices of private sector organizations. The Privacy Commissioner is also mandated to assist organizations and individuals with understanding the legislation, and to undertake research on issues pertinent to information privacy.

Observers agree that one factor motivating the development of the *Personal Information Protection and Electronic Documents Act* was the changing international environment with respect to information privacy. In the last 20 years, concerns about information privacy in private sector transactions has grown into a significant policy issue in Canada and around the world. For example:

- In 1980, the Organization for Economic Cooperation and Development adopted its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines), which set out widely accepted minimum standards for the use of personal data. Canada became a signatory to the OECD guidelines in 1984.
- The province of Quebec has had privacy protection legislation in place for the private sector since 1994, when it passed *An act respecting the protection of personal information in the private sector* (Loi sur la protection des renseignements personnels dans le secteur privé).[9] In addition, the *Quebec Charter of Human Rights and Freedoms*, effective since 1975, recognizes privacy as a human right. Since 1991, Quebeckers have also been guaranteed the right to privacy through

the *Quebec Civil Code*. Observers note that with these three measures, Quebec provides its citizens with the most comprehensive range of privacy rights of any Canadian jurisdiction.[10]

- During the 1990s, consumer, industry and labour representatives, privacy advocates and legislators cooperated on the development of a voluntary Canadian privacy standard for the private sector, which resulted in the 1996 Canadian Standards Association Model Code for the Protection of Personal Information (CSA Model Code).
- The European Union's 1998[11] *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) guarantees that citizens of all European Union (EU) member states will receive equal protection of their personal information.

The EU Directive is the most influential of those developments, because it regulates the privacy protection of all data transfers to and from EU member states. The Directive requires EU member nations to limit external data exchanges to only those jurisdictions that have established adequate data protection rules. The *Personal Information Protection and Electronic Documents Act* is Canada's response to the EU Directive, and is meant to ensure that data will continue to flow freely between Canadian and European enterprises.

Another motivating factor was the need for Canada to compete in the global electronic commerce (e-commerce) environment. In 1999, Canada held approximately 6 percent of the $195.39 billion (CDN) global e-commerce market.[12] Global e-commerce is expected to generate almost 4 trillion (CDN) by 2004, and Canada is now well positioned to increase its portion of that market.[13] Statistics Canada reports that the Canadian government is "reaching its goal to 'make Canada the most connected nation in the world'", but must continue to foster the implementation and use of e-commerce in all economic sectors, especially among small to medium-sized enterprises.[14] Canada's Electronic Commerce Strategy, designed to create a favourable environment for the growth of e-commerce, established the protection of information privacy for the private sector as a key component of the strategy. As then Privacy Commissioner of Canada noted in 1998,

> *The government has recognized that a knowledge-based economy is driving global growth and is determined to make Canada "the most connected nation in the world." And it wants to create an environment which will see Canada out in front of the pack in developing electronic commerce.... However, the government also understands that they have to build trust in the system, many Canadians will not shop, bank and file taxes on line....* [15]

Finally, the development of the CSA Model Code demonstrated to government that Canadian consumers, businesses and legislators could agree on an acceptable model for the protection of personal information in business transactions.

British Columbia is faced with circumstances similar to those that brought about the *Personal Information Protection and Electronic Documents Act*. E-commerce has influenced all activities in the private sector: businesses in this province are, like those throughout the information economy, dealing with buyers, suppliers and employees spread across national and international jurisdictions, linked through information technologies. A 1998 survey of BC businesses showed that 97 percent were using the Internet in their business operations. The three most important e-commerce activities they identified were the promotion of products and services to potential consumers, the purchase of products and services, and pre- or post-sales support. Most also expressed their intention to develop direct-to-customer online sales as part of their business strategies.[16]

In this integrated economic environment, British Columbia businesses are affected by the standards established by other jurisdictions with which they do business. In the case of information privacy, this means that British Columbia must decide how to meet the challenge of the federal *Personal Information Protection and Electronic Documents Act*, similar legislation enacted or to be enacted in other Canadian provinces, and the international regulatory environment.

While the BC *Freedom of Information and Protection of Privacy Act* has, since 1993, safeguarded the privacy of personal information held by government bodies, personal information collected, used and disclosed by private sector businesses and organizations is not protected by privacy legislation. To demonstrate the reach of private sector entities in this province that are not subject to information privacy law, the former Information and Privacy Commissioner of British Columbia, David Flaherty, provided this non-exhaustive list:

> *...telephone companies... trust companies, credit unions, employer associations, labour unions, transportation and telecommunication companies, large and small retailers, grocery stores, pharmacies, direct marketers, telemarketers, credit reporting bureaus, insurance companies and brokers, physicians, dentists, lawyers, accountants, therapists, psychologists, travel agencies, charitable organizations, associations, churches, hotels, investment dealers, the media, and video rental shops.*[17]

Some others include independent schools, children's daycares, private post-secondary institutions, fitness centres, car dealerships and private sector employers. Essentially, it includes any private sector enterprise not designated a federal responsibility under Canada's constitutional division of powers.

THE INFORMATION ECONOMY

The emergence of information privacy as a public policy issue is attributed to economic globalization, rapid developments in information technology, and the growth of e-commerce, which have in turn led to an increase in public concern about information privacy in business transactions. We are now living in what commentators call "the information society"[18] and participating daily in a globalized "information economy," which is characterized by information as a driver of economic growth, the increased use of information technologies, and business conducted with fewer limitations imposed by political or territorial boundaries.

The information economy refers to the transformation of society out of the industrial age, which focussed on the movement of people and goods, into an economy based on information, which includes both data and ideas in text, audio and video formats. In information economies, information exchanges take the place of various material transactions, as in electronic banking, for example, or the maintenance of customer databases rather than paper files. The volume of information and the value of information are increased, as information technologies can combine or otherwise process raw information in ways that allow it to reveal its latent intelligence.

Information technologies are technologies that emerged during the last 20 years from the development and fusion of two previously distinct technologies: digital computing and telecommunications. The resulting mechanisms have been described as "an interactive system of multipurpose technologies" designed around information usage.[19] The common link between all types of information technologies is their ability to "understand" digital data, which is information that has been translated into binary code. Information in any form - text, sound, image, or video - can be digitized, and then read by any computer system, whether the system is designed for information storage, processing, or transmission to other computers.

Information technologies have enabled users to create, access, store, retrieve and transmit large amounts of data quickly and almost unhindered by geographical location and traditional means of transport. In this respect, information technologies are themselves a globalizing influence, allowing digitized information to be transferred among technology users in all parts of the world. In a globalized business environment, a company may collect customer data in one country and process the data in another country. It may use the services of another company for data storage and maintenance, or it may sell goods and services to distant customers.

At the same time that the information processing and transmission power of information technologies has increased, relative cost of these technologies has rapidly declined. Increased processing power, lower equipment costs, and the ease and cost-efficiency of handling digitized information as compared to nondigital data have all been used to explain the rapid diffusion of information technologies into all parts of life, including the personal, governmental, commercial, health, and educational spheres.[20] The diffusion of information technologies throughout society also means that the information economy encompasses businesses of all sizes, from small, local enterprises to multinational companies.

As mentioned, e-commerce has emerged as an important force in the information economy. Electronic commerce can be defined as "the conducting of business transactions through technology enabled communication with customers and suppliers."[21] It includes technologies ranging from fax and e-mail, to consumer point-of-sale technology, to computer-to-computer Electronic Data Interchange and the Internet. Companies have successfully networked their development, production and distribution operations to streamline inventory. They have also adopted information technologies to simplify their sales and billing processes. Consumers have also adapted readily to the electronic business environment. Convenience - speed and easy access to products, services and information - as well as incentives like "loyalty" discounts and "points" have made electronic transactions popular with consumers.[22]

INFORMATION TECHNOLOGIES

Compared to paper-based records, personal information recorded electronically can be collected, processed, stored and transmitted relatively cheaply in a multitude of ways that were unthinkable even a decade ago. And, in the information economy, personal information is a valuable commodity. The expansion of the marketplace and the increased use of electronic communications have attenuated the relationships between businesses and their customers or clients. When businesses and customers did business face-to-face and were well known to each other, merchants learned their customers' preferences and earned their trust by the relationships they built up over time. Businesses could also consider those relationships in evaluating business risks, such as the risk involved in extending credit to a customer. In an information economy, there are fewer opportunities to build those kinds of relationships. Businesses are now using the personal information they collect about consumers in order to reproduce the kind of knowledge and trust that business relationships can provide. The value of personal information in the information economy is so great that customer data is considered an important resource.

For example, personal information is used extensively in marketing. Consumers today have access to a large number of businesses and service providers; consequently, competition for consumer dollars is intensified. Personalized service is one strategy used by many businesses to gain a competitive advantage. The focus of marketing has therefore changed from mass marketing - advertising directed at the public at large - to customer-centred, preference-based marketing.[23] Preference-based marketing is used widely in the private sector: retail stores, financial service providers, and even television stations and magazine publishers cater to the defined market segments they have discovered by analyzing consumer information to find out who their customers are, what characteristics they share and what products or services they want.

Many ordinary business transactions allow business to collect personal information about consumers. Some businesses ask customers for their telephone numbers, addresses, driver's licence numbers, or social insurance numbers. Consumers provide personal information to businesses just by:

- Subscribing to a magazine
- Filling out a warrantee form
- Filling out a contest entry form
- Taking out a bank loan
- Taking out insurance policies or making claim on their policies
- Making a charitable donation
- Renting a car
- Staying at a hotel
- Flying on a commercial airline
- Purchasing a house, condominium or property

Businesses can also collect information automatically and invisibly using digital technologies. The following list shows a few of the common business transactions that involve the electronic identification of individual consumers and the collection of their personal information:

- Banking through automated teller machines
- Paying with debit cards or credit cards
- Using customer loyalty cards, such as air miles or "club" cards
- Renting videos
- Making telephone calls
- Sending e-mail
- Browsing the Internet

Electronic collection methods are some of the most effective, but consumers are often unaware that they are providing it, or at least, how much information they are disclosing.

Internet technology in particular enables web site operators to quietly collect a wealth of personal information about Internet users. Internet "cookies", for example, allow web site operators to track Internet users' browsing habits without their knowledge or consent. Cookies are text files transferred to Internet users' computers by the web pages they view. When a viewer's computer loads a web page, the page sends the cookie file, which contains an identification number, and saves it in the user's browser program in a designated folder. When the user visits another page on the same web site, or visits the same page again, the information contained in the cookie file is transferred back to the site, enabling it to "remember" what the user viewed previously.

Non-persistent cookies are often used on e-commerce sites to allow the site to maintain a "shopping cart" for Internet users. Session or non-persistent cookies are maintained by the user's browser only for the duration of a single Internet session. When the user ends his or her Internet session, the non-persistent cookies expire.

Persistent cookies are stored on the user's hard-drive for much longer periods of time - sometimes more than two years - enabling the web site to recall a user's transactions from various Internet sessions. Persistent cookies are often used to assist site operators in assessing and improving their web sites by tracking how many times individual computers have accessed particular pages on their sites. Cookies are also used to customize users' start pages and registrations on sites that require a password. For example, when a user chooses to use a site as his or her homepage, he or she can indicate a preference for particular topics to be displayed on the page. Or, a user that has registered to use an online media site can personalize the headlines they are shown when they enter the site. Cookies will also remember the passwords of registered site users.

However, the information gathered by cookies may also be used to develop detailed profiles of users and their browsing habits. Some web sites exist only to collect personal information for advertising purposes. Banner advertisers have exploited the possibilities provided by cookies by partnering with web site operators and using persistent cookies to follow individual users' transactions across all participating sites. This allows banner advertisers to collect create a more comprehensive profile of a user's preferences by logging many of the Internet sites he or she visits. Based on the user's viewing profile, the banner advertiser's cookie determines what ads will be of special interest to the user so that personalized banner ads can be placed at the top of each page he or she views.

Once personal information has been collected, manually or automatically, it can easily be stored, processed or transmitted using information technologies. Database technologies allow for all three: they are automated collections of data that allow data to be input, stored, retrieved, shared, edited, sorted and queried. Databases are organized so that the data from one can easily be incorporated into or read by another database. They are sometimes connected to a computer network, so that employees in a distributed business environment can use the same database for any function no matter where they are located. In this sense, "[d]atabases, despite their dispersed and decentralized structure, form a more or less unified functional system."[24] Databases are also capable of performing complex information processing functions that enable businesses to increase the value of raw consumer data. Two processes that are widely used in the private sector are data matching and data mining.

Data matching is a process of linking separate and previously unrelated pieces of information about the same person. Using data matching, businesses can find out which of their customers are higher risks, or a good candidates for a new product. For example, a retailer might match its customer database against a database containing purchases made from the competition in order to see what products or services it should improve or expand.

Private sector databases typically contain personal information that consumers and clients have provided to businesses and organizations, either with or without their knowledge and consent. Some of that information is not considered personal information because it does not identify a particular individual. However, with data matching, even data that is anonymous at the time of collection can be transformed into personal information. For example, by linking databases of Internet users' information with customer information databases - which are more likely to contain identifiable personal information like names, phone numbers and/or addresses - businesses can create profiles of identifiable individuals' interests and preferences based on both their consumer behaviour and their Internet browsing habits.[25]

Data mining is another commonly used way of processing consumer information to add-value. Data mining uses artificial intelligence to uncover unknown patterns or relationships in large data sets that can be used to predict consumer behaviour. In effect, it creates new personal information from the personal information originally obtained from consumers. Data mining allows businesses to discover:

- what types of products are typically purchased together
- how purchases are associated sequentially; for example, purchases that are likely to follow the purchase of a house
- what demographic "types" of consumers buy certain products
- how consumer types are likely to behave; for example, data mining can be used to predict which customers are likely to default on payment, due to bankruptcy or for other reasons
- anomalous credit card usage, which may indicate that the card has been stolen
- irregularities in data that could signify data entry errors[26]

Data mining gets the most accurate results from analyzing the recurrence of patterns in large amounts of information, so businesses using data mining applications often gather consumer information gathered from diverse sources. Data mining applications in the private sector need cumulative transactional data, sometimes gathered over periods ranging from six months to two years, including information gathered from credit card records, customer lay-away plans, preferred customer programs, frequent shopper clubs, or survey samples.[27] They also need non-commercial information about customers, which might consist of demographic (age, gender, and martial and family status), economic (salary level, occupation, and household income), or geographical data (province, city, street or postal code area).[28]

The Privacy Commissioner of Ontario has identified a number of privacy concerns with data mining: it is generally based on the secondary use of personal information, for which informed consent has likely not been provided; by its very nature - knowledge discovery - data mining cannot ensure that personal information is used for limited, defined purposes; it lacks transparency; and it does not allow consumers the opportunity to access or request corrections to the personal information created through data mining.[29]

Other commentators have suggested that information technologies like data mining have the potential to restrict the ability of individuals to define themselves in relation to business. The personal information residing in private sector databases can function as so many "virtual selves" that inadequately represent the real individual in businesses' assessments and decisions. The long-term effect, these observers warn, could be "data predestination", where personal data becomes "a self-fulfilling prophecy, defining the sort of offers that you receive, your credit opportunities, your school choices... . When the scope of your future is limited by information in your profile at each step of your life."[30] Furthermore, "[g]iven a dispute between this virtual self and the actual individual, who is to be believed?"[31]

In summary, information technologies allow for the collection, use, storage or transmission of large amounts of customer information from diverse sources, and the creation of new data about customers. In terms of information privacy, information technologies' major drawbacks are their lack of transparency: consumers are unlikely to know what information has been collected, what information exists, who has it, where to find it, or how to check it or have errors corrected. Consumers should at least be aware that private sector businesses and organizations can accumulate and analyze large amounts of their personal information, and that the information they provide may end up in a form that is more than the sum of its original parts.

INFORMATION PRACTICES IN BC'S PRIVATE SECTOR

Private sector businesses and organizations use personal information for many legitimate business purposes. As mentioned, personal data is necessary for assessing business risks. Private sector businesses may need to evaluate an individual's suitability for credit, insurance, or employment. For example, when buying insurance, an individual must provide some personal information to help the insurer determine his or her risk level, and therefore what premium should be charged. Indeed, the Canadian Life and Health Insurance Association prefaced its remarks to the Committee by noting that personal information - financial information, health information, information on family relationships - is the "raw material" of the life and private health insurance industry and is vital to its functioning.[32] Using customer data, businesses also determine how to improve sales with established customers, learn how to improve products and services, decide which new products to develop, and discover where they are likely to find new customers.

The Committee heard that British Columbia's private sector businesses and organizations vary widely in the type and amount of personal information collected from consumers. While some collect only the names and addresses of customers or clients, and others record consumer transactions for billing or shipping purposes, some collect "quite detailed and highly personal information," and some collect personal information for purposes other than fulfilling the original transaction[33]:

- In direct marketing or relationship-management with current customers, personal information is used for informing customers or clients about new products, special offers or sales, or customer rewards. Businesses see these activities as ways of building relationships with customers or clients, improving customer service, and therefore holding onto customers against the competition. Some businesses believe their customers want the personalized service that direct marketing offers, and some give their customers the choice to opt-out of direct marketing or relationship management programs.[34]
- Detailed consumer profiles do not need to contain identifying information to be useful to businesses. Sometimes, all business need is aggregated data about their customers or the market for their goods and services. Business participants reported that they generally analyze aggregate data to see overall patterns of consumer behaviour, such as frequency, transaction types and geographic location, so that they can prepare marketing strategies or make real estate decisions.[35]
- *"Companies with loyalty programs tend to regard their membership databases as 'gold' – in other words, they are an investment to be carefully guarded."* These companies use contact information internally for promotions and coupons, customer satisfaction research, and direct marketing, but do not share their lists with other companies. Managers of these programs felt strongly that consumers want and expect consumer "rewards", and that therefore, loyalty programs are essential.[36]
- Those involved in direct marketing, list-brokering and telemarketing also see consumer information as an investment. But unlike others, they also view it as a commodity to be bought or sold. Their use of personal information is typically quite complicated, involving many different parties. E-mail is a method commonly used to transmit consumer lists, and encryption is not always used to protect the data.[37]
- The amount and type of information collected by credit unions varies depending on the type of product or service: *"A simple savings account requires much less information than a mortgage application would; however, even equipping a member to use ATM machines requires a credit check*

to determine appropriate daily withdrawal maximums. At most, information gathered can include full information on credit history, full information on all financial assets and debt, all sources of income, as well as personal contact information." In addition, credit unions may collect members' information from their use of online banking services, and may process members' information using "customer relationship management systems", which "organize and track" clients' transactions and interactions with customer service personnel.[38]

- Charities have to carefully weigh potential costs and benefits before deciding whether or not to share their donor lists. By sharing their donor lists or membership lists with other organizations, charities can effectively expand their donor bases, but it is risky, since current donors might stop giving in order to prevent their names and addresses from being passed on to others. Some charities, because they believe that many of their supporters want privacy, do not trade or sell donor lists to other organizations. They may instead offer newsletters and membership in the organization as a way of encouraging donors to donate regularly or at higher levels.[39]
- Residential property managers hold some very detailed personal information about applicants and tenants. Tenancy application forms and residential tenancy agreements typically request the applicant's or tenant's full name; date of birth; social insurance number; current address, phone and postal code; employer's name and address; next of kin's name and address; names and ages of all persons who will be residing in the home; and length of time at current residence, whether it is rented or owned, landlord's name and phone number, and reason for leaving. Tenancy application forms may also request the following as optional information or may require it if other information is not provided, although forms don't always state that it is optional: fax number; email address; marital status; drivers license number; insurance for third-party liability or personal belongings; income, position, length of employment, and information about previous employment; name, phone number and location of the applicant's financial institution, types of accounts, and account numbers; credit card company and credit card number; and automobile ownership, including make, model, license plate number and colour.[40]

The Committee also heard that some private sector organizations and businesses take great care to protect the information privacy of their customers and clients. Private sector businesses and organizations are well aware of their the public's privacy concerns, and believe that appropriate information handling practices are therefore essential to the viability of their businesses:

> *On many separate occasions, business representatives mentioned their obligation to treat personal information with "respect"…:*
>
> - *"Everyone is tired of getting twenty different subscription offers."*
> - *"When customers provide us with certain pieces of information, they generally understand that we are going to use that information [internally]."*
> - *"The kind of detail about the customer that is revealed through their purchases can be quite personal. If a customer has honored you by entrusting you with their personal information, you have to respect that."*
> - *"Our database is our bread-and-butter, and we treat it with respect."*[41]

Many have therefore adopted information handling practices that they believe will satisfy their customers, clients, members, donors and employees. In order to respect individuals' privacy, businesses and organizations reported observing three general practices:

Limit external distribution of information:
Organizations recognize that the most important element of protecting consumer privacy is never sell or trade consumer lists with third parties without the consumer's consent. (Notably, this does not rule out reaching out to current customers through direct marketing campaigns, or buying lists from list brokers in order to try to grow their customer or donor base.) Several organizations mentioned they do not even disclose personal information to family members or to police officers (unless they have a warrant). This rule was observed by all companies and professionals included in our study except those in the direct marketing sector. Naturally, companies whose business is in list-brokering or lead-generation (telemarketing) don't balk at passing on consumers' personal information, as that information is the product in which they trade; but interestingly, these companies are often very careful about not disclosing information about their actual clients.

Limit internal access to information:
It is quite common for organizations to allow access to personal information only to those employees who need to see it to do their job; for example, only those who are fulfilling orders, billing customers, or dealing directly with the customer will have access to the customer's purchase or address information. Other people in the company would have access to aggregated non-personal information about the customer base. This rule is regarded as less critical than limiting external distribution, and not all organizations are large enough to warrant a systematic or formal application of this principle. (In a small office, it may be a matter of only one or two people having access to the computer or the filing cabinet which holds the information.) However, it is fairly common for businesses, whether large or small, to observe a policy of limited internal access to personal information. The larger the company the more likely it is to have a formalized system of limited access.

Limit collection or retention of information:
One online retailer asked only for the basic information needed to deliver the product and had labeled the few other non-essential information areas (such as age, gender) as optional. Other companies do gather fairly detailed transactional or other information, but keep it only as long as required for the purposes related to that transaction and shred or delete much of it quite quickly. This rule is one that not every company follows: some ask for a large amount of detailed, "extra" information (whether labeled as optional or not); others need to gather it for the purposes of the transaction, but may also study it or use it for marketing purposes.[42]

Private sector businesses and organizations also use other methods to protect the privacy of personal information. They mentioned keeping personal information in separate databases; defining levels of access within databases to limit employee access to personal records; using firewalls or stand-alone systems to secure computerized data from external access; and using reliable encryption technologies for online business transactions. "Low-tech" methods, like locking doors and cabinets and shredding records, were also mentioned.[43]

Some larger companies and industry associations have designated internal privacy authorities or developed privacy codes. The Committee heard that the Canadian Marketing Association was one of the original members of the Canadian Standards Association Technical Committee, which developed the CSA Model Code. The Association has had a mandatory privacy code for its members since 1993, which is being updated to conform to the federal *Personal Information Protection and Electronic Documents Act.*[44] The Professional Marketing Research Society has developed standards codes for its members that are designed to encourage ethical conduct, and include standards for privacy protection based on the CSA Model Code.[45] In 1992, the Insurance

Bureau of Canada's *Model Privacy Code for the Individual Insurance Customer* was approved by the Bureau and adopted by more than 80 percent of its member companies. In 1996, the Bureau's updated privacy code -- the *Model Personal Information Code* - received CSA approval.[46] The Canadian Bankers Association was involved in the development of the CSA Model Code, and in 1996, the Association's own privacy was independently confirmed as complying with the CSA standard.[47]

However, the Committee also learned that,

> *in general, only larger companies have designated information privacy officers and a written policy on information privacy.... Many smaller organizations have informal policies, communicated to employees verbally, but do not have a written set of guidelines available to consumers. Companies that do business online generally do have a set of written privacy policies posted on their web sites (although, it is possible that these guidelines pertain only to the online portion of their business; the traditional portion of their business may not be covered).*[48]

In conclusion, businesses are aware that it is good business to protect the privacy of personal information. Nonetheless they also report that privacy doesn't appear to be an pressing issue for their customers and clients: "Few mentioned getting feedback from customers about their privacy practices; some therefore concluded that the consumers they deal with are fairly comfortable with the way their personal information is handled."[49]

BRITISH COLUMBIANS' VIEWS ON INFORMATION PRIVACY

Most British Columbians – 73% – express at least moderate concern about the issue of information privacy, while 3% say they are not at all concerned about the issue.[50]

Of those British Columbians who are concerned,

- *18% are concerned about their information being sold to direct marketers.*
- *9% dislike the idea of "big brother" knowing too much about them.*
- *4% worry that there is the potential for information to be used against them in some way.*[51]

Concern about the privacy of personal information on the Internet was consistent, at 12 % in the concerned group, and 10 % in the unconcerned group.[52]

The Committee heard that while the privacy of personal information is not an urgent concern, British Columbians are definitely uneasy about their personal information being collected, used, disclosed and retained. They are also aware of the amount, frequency and sensitivity of the personal information businesses and organizations obtain from them.[53] Some expressed concern that consumers are defenseless against unauthorized collection, use and disclosure in consumer-to-business and business-to-business operations, including direct marketing, loyalty programs, credit reporting, Internet technologies, fraud and "scams". Some people noted that "technology challenges information privacy because it makes gathering, organizing, and transferring information a quick and easy process."[54] In view of the wide range of businesses and organizations that have and use personal information, one individual told the Committee that legislators must acknowledge "the scope and diversity of assaults on personal privacy."[55]

Some people expressed a general sense of unease at the idea that their information privacy could be compromised by "someone finding out a lot about you", or by computer hackers.[56] This sense was not so much related to the harms that might occur if personal information is misused, but arose

Bureau of Canada's *Model Privacy Code for the Individual Insurance Customer* was approved by the Bureau and adopted by more than 80 percent of its member companies. In 1996, the Bureau's updated privacy code -- the *Model Personal Information Code* - received CSA approval.[46] The Canadian Bankers Association was involved in the development of the CSA Model Code, and in 1996, the Association's own privacy was independently confirmed as complying with the CSA standard.[47]

However, the Committee also learned that,

> *in general, only larger companies have designated information privacy officers and a written policy on information privacy.... Many smaller organizations have informal policies, communicated to employees verbally, but do not have a written set of guidelines available to consumers. Companies that do business online generally do have a set of written privacy policies posted on their web sites (although, it is possible that these guidelines pertain only to the online portion of their business; the traditional portion of their business may not be covered).*[48]

In conclusion, businesses are aware that it is good business to protect the privacy of personal information. Nonetheless they also report that privacy doesn't appear to be an pressing issue for their customers and clients: "Few mentioned getting feedback from customers about their privacy practices; some therefore concluded that the consumers they deal with are fairly comfortable with the way their personal information is handled."[49]

BRITISH COLUMBIANS' VIEWS ON INFORMATION PRIVACY

Most British Columbians – 73% – express at least moderate concern about the issue of information privacy, while 3% say they are not at all concerned about the issue.[50]

Of those British Columbians who are concerned,

- *18% are concerned about their information being sold to direct marketers.*
- *9% dislike the idea of "big brother" knowing too much about them.*
- *4% worry that there is the potential for information to be used against them in some way.*[51]

Concern about the privacy of personal information on the Internet was consistent, at 12 % in the concerned group, and 10 % in the unconcerned group.[52]

The Committee heard that while the privacy of personal information is not an urgent concern, British Columbians are definitely uneasy about their personal information being collected, used, disclosed and retained. They are also aware of the amount, frequency and sensitivity of the personal information businesses and organizations obtain from them.[53] Some expressed concern that consumers are defenseless against unauthorized collection, use and disclosure in consumer-to-business and business-to-business operations, including direct marketing, loyalty programs, credit reporting, Internet technologies, fraud and "scams". Some people noted that "technology challenges information privacy because it makes gathering, organizing, and transferring information a quick and easy process."[54] In view of the wide range of businesses and organizations that have and use personal information, one individual told the Committee that legislators must acknowledge "the scope and diversity of assaults on personal privacy."[55]

Some people expressed a general sense of unease at the idea that their information privacy could be compromised by "someone finding out a lot about you", or by computer hackers.[56] This sense was not so much related to the harms that might occur if personal information is misused, but arose more from the idea that privacy is germane to personal identity.[57] For example, one individual explained, "I would never want just anybody to know who, what, why and wherefore I am." [58]

Another group said that information privacy is every individual's right. For example, one individual wrote:

> *My information belongs to me. I want to control it, how it is being used and to whom it is being released. Individuals and corporations are controlling my personal information and realizing profit from it. This is unjustifiable and must cease.*[59]

Still others are mainly annoyed that the use of personal information in the private sector results in a "barrage of direct mail." In these cases people have negative feelings about the original transaction in which their information was collected, and the direct marketing transactions that result from the sharing of their information.[60]

Some are simply resigned to the idea that they provide their personal information to businesses and organizations in order to obtain the products and services they want, and are not in the habit of asking why it the information is needed. If getting junk mail is the only result, it's okay with these people: "it is necessary to businesses and largely benign to consumers."[62]

29% of those who expressed concern about information privacy also said that people have a right to privacy.

26% of those who expressed concern about information privacy said they feel that they lack control over their personal information.[61]

Whatever their personal feelings about businesses' information practices, individuals reported taking some steps to protect their information privacy. They will sometimes refuse to give particular pieces of information, like social insurance numbers; they use variations on their names when subscribing to catalogues or magazines; fill out forms incompletely or provide false information; register only with web sites they trust; and will not make online purchases.[63]

A clear minority of individuals, businesses and organizations are unconcerned about informational privacy in private sector transactions. Some feel that privacy is an issue that has been "hyped" by the media, which focuses on privacy horror stories.[64] But "the majority of those who say they are not particularly worried about information privacy say it is because they simply have nothing to hide"; that is, of those who are neutral about the issue, 21 percent said they "have nothing to hide", and of those who are unconcerned, 50 percent gave that reason.[65]

The Committee also heard about the kinds of information British Columbians believe are most sensitive from a privacy point-of-view. Some expressed concern about the privacy of personal information used by charitable organizations, the media, and landlords. Other believe that specific types of personal information need privacy protection against private sector usage, including children's information, employee information and financial information. British Columbians are most concerned about the privacy of financial and health information. When asked how important it is that financial information be kept private, 89 percent said it is "very important". In response to the same question about medical or health information, 76 percent of respondents said very important; about Internet usage information, 52 percent said very important; about employment records, 51 percent said very important, and about shopping habits, 28 percent said very important.[66]

Even publicly available information, like name, address and phone number, is considered sensitive by some people. One person objected to business disclosures of personal information to third parties for direct marketing purposes, and particularly disclosures of personal information collected through seniors' discount offers. In her view, seniors are especially vulnerable to direct marketing techniques, and must be protected from targeted marketing based on personal information collected or disclosed through seniors discount programs.[67] Another wrote that third-party access to unlisted phone numbers and addresses leaves some individuals at risk, such as women who are estranged from violent partners, abortion service providers, and others. He believes that advertisers can easily access addresses and phone numbers, even unlisted ones, and is concerned that private investigators are able to obtain personal information for clients whose motives are questionable. While 55 percent of British Columbians overall think the privacy of this information is important, women are significantly more likely than men to say that this information must be kept private: "[n]early half of women assign the highest possible level of importance to keeping their identifying information private (47 percent assigned a score of 7 on the 7 point scale, compared with just 33 percent of men)."[68]

EMPLOYEE INFORMATION

Employers and potential employers collect a great deal of personal information about employees and prospective employees. When applying for a job, individuals generally provide standard information to the potential employer:

- *Last, first, and middle names*
- *Phone numbers*
- *Present and previous addresses, and how long lived at each*
- *Education level*
- *Position applying for*
- *Availability*
- *Employment history (Company name and address, last position, leaving salary, time there, and reason for leaving)*
- *Specific skills*[69]

This information, and reference checks, are indispensable to the business or organization in determining the applicant's suitability for the job. Private sector employers reported that:

> *[h]uman resource officers keep employee information under strict lock and key. Files are accessible by only a few people in the organization and electronic files are stored and processed by a dedicated server. Concern about the security of private information among employees is limited because of these precautions. The only questions asked in this regard have had to do with access to one's own file.*[70]

Businesses noted that the information collected on unsuccessful applicants is normally disposed of in less than a year.[72]

51% of British Columbians believe it is "very important" that employment records be kept private, and 12% said it is "not at all important" that they be kept private.[71]

The Committee also heard individuals, businesses and organizations say that private sector employees in British Columbia do not have adequate privacy protection for their personal information. One organization told the Committee that it frequently hears complaints that employers intrude upon employee privacy with employment application requirements, psychological testing, drug testing, access to employee health information, searches through personal effects, video and audio surveillance, and computer monitoring. It was also noted that electronic surveillance technologies have made it increasingly possible for employers to monitor employees, using closed-circuit television systems, keystroke monitoring, computerized more from the idea that privacy is germane to personal identity.[57] For example, one individual explained, "I would never want just anybody to know who, what, why and wherefore I am." [58]

Another group said that information privacy is every individual's right. For example, one individual wrote:

> *My information belongs to me. I want to control it, how it is being used and to whom it is being released. Individuals and corporations are controlling my personal information and realizing profit from it. This is unjustifiable and must cease.*[59]

Still others are mainly annoyed that the use of personal information in the private sector results in a "barrage of direct mail." In these cases people have negative feelings about the original transaction in which their information was collected, and the direct marketing transactions that result from the sharing of their information.[60]

Some are simply resigned to the idea that they provide their personal information to businesses and organizations in order to obtain the products and services they want, and are not in the habit of asking why it the information is needed. If getting junk mail is the only result, it's okay with these people: "it is necessary to businesses and largely benign to consumers."[62]

29% of those who expressed concern about information privacy also said that people have a right to privacy.

26% of those who expressed concern about information privacy said they feel that they lack control over their personal information.[61]

Whatever their personal feelings about businesses' information practices, individuals reported taking some steps to protect their information privacy. They will sometimes refuse to give particular pieces of information, like social insurance numbers; they use variations on their names when subscribing to catalogues or magazines; fill out forms incompletely or provide false information; register only with web sites they trust; and will not make online purchases.[63]

A clear minority of individuals, businesses and organizations are unconcerned about informational privacy in private sector transactions. Some feel that privacy is an issue that has been "hyped" by the media, which focuses on privacy horror stories.[64] But "the majority of those who say they are not particularly worried about information privacy say it is because they simply have nothing to hide"; that is, of those who are neutral about the issue, 21 percent said they "have nothing to hide", and of those who are unconcerned, 50 percent gave that reason.[65]

The Committee also heard about the kinds of information British Columbians believe are most sensitive from a privacy point-of-view. Some expressed concern about the privacy of personal information used by charitable organizations, the media, and landlords. Other believe that specific types of personal information need privacy protection against private sector usage, including children's information, employee information and financial information. British Columbians are most concerned about the privacy of financial and health information. When asked how important it is that financial information be kept private, 89 percent said it is "very important". In response to the same question about medical or health information, 76 percent of respondents said very important; about Internet usage information, 52 percent said very important; about employment records, 51 percent said very important, and about shopping habits, 28 percent said very important.[66]

Even publicly available information, like name, address and phone number, is considered sensitive by some people. One person objected to business disclosures of personal information to third parties for direct marketing purposes, and particularly disclosures of personal information collected through seniors' discount offers. In her view, seniors are especially vulnerable to direct marketing techniques, and must be protected from targeted marketing based on personal information collected or disclosed through seniors discount programs.[67] Another wrote that third-party access to unlisted phone numbers and addresses leaves some individuals at risk, such as women who are estranged from violent partners, abortion service providers, and others. He believes that advertisers can easily access addresses and phone numbers, even unlisted ones, and is concerned that private investigators are able to obtain personal information for clients whose motives are questionable. While 55 percent of British Columbians overall think the privacy of this information is important, women are significantly more likely than men to say that this information must be kept private: "[n]early half of women assign the highest possible level of importance to keeping their identifying information private (47 percent assigned a score of 7 on the 7 point scale, compared with just 33 percent of men)."[68]

EMPLOYEE INFORMATION

Employers and potential employers collect a great deal of personal information about employees and prospective employees. When applying for a job, individuals generally provide standard information to the potential employer:

- *Last, first, and middle names*
- *Phone numbers*
- *Present and previous addresses, and how long lived at each*
- *Education level*
- *Position applying for*
- *Availability*
- *Employment history (Company name and address, last position, leaving salary, time there, and reason for leaving)*
- *Specific skills*[69]

This information, and reference checks, are indispensable to the business or organization in determining the applicant's suitability for the job. Private sector employers reported that:

> *[h]uman resource officers keep employee information under strict lock and key. Files are accessible by only a few people in the organization and electronic files are stored and processed by a dedicated server. Concern about the security of private information among employees is limited because of these precautions. The only questions asked in this regard have had to do with access to one's own file.*[70]

Businesses noted that the information collected on unsuccessful applicants is normally disposed of in less than a year.[72]

The Committee also heard individuals, businesses and organizations say that private sector employees in British Columbia do not have adequate privacy protection for their personal information. One organization told the Committee that it frequently hears complaints that employers intrude upon employee privacy with employment application requirements, psychological testing, drug testing, access to employee health information, searches through personal effects, video and audio surveillance, and computer monitoring. It was also noted that electronic surveillance technologies have made it increasingly possible for employers to monitor employees, using closed-circuit television systems, keystroke monitoring, computerized

51% of British Columbians believe it is "very important" that employment records be kept private, and 12% said it is "not at all important" that they be kept private.[71]

surveillance of vehicle use, tracking of employee location, and monitoring of telephone, Internet, and e-mail use.

Two points of view were evident in the discussion of workplace surveillance. On the one hand, surveillance contributes to workplace stress, a loss of dignity and diminished trust. Employees' may consent to surveillance practices, but in the workplace, it is difficult to ensure that consent is given freely:

> *The reality of many employees, needing work in a time of high unemployment and the relative difference in power, means that notice and consent are not enough to adequately protect employee privacy.... Employees must be able to raise their concerns with an independent arbitrator regarding employer practices.*[73]

BC's Information and Privacy Commissioner, David Loukidelis, surmised that due to the contractual relationship between employer and employee, people believe that employers have the right to monitor their employees. However, the Commissioner maintains that just as the *BC Human Rights Code* applies in the workplace and guarantees certain protections for employees,

> *[i]f we accept that privacy is more than merely an economic right...., it seems to me that the analysis of appropriate workplace practices has to include the possibility – and indeed ... desirability – that restrictions on an employer's right to undertake monitoring of employees are appropriate.... We already regulate...how employers behave towards their employees when it comes to issues like discrimination on the basis of sex, sexual orientation, race and so on.*[74]

On the other hand, some argued that employers have a legitimate need to make sure that employees maintain the security of business information, do not behave in ways that will make the company liable for the employee's actions, and to maintain the security of their computer systems to avoid costly system crashes.[75] One individual agreed that monitoring employees can reduce an employer's legal responsibility for employees' misbehaviour, (like browsing the Internet for illegal materials or sending hate mail), but suggested that there are more ethical ways of achieving the same end.

HEALTH INFORMATION

Personal health information is considered one of the most sensitive forms of personal information. It includes the kinds of information an individual gives his or her doctor for the purposes of receiving treatment, from name, address, and health insurance number, to information about physical condition, emotional state, personal habits, sexual practices, medication, and family history, and information that physicians record on patient records in the course of providing care, like diagnoses, prescriptions progress reports and opinions.[76]

Health information is not only collected and used by medical doctors and dentists, but also by counsellors, psychologists and other therapists. Health information collected and used by these professionals may include sensitive information about family dynamics, substance abuse and mental health issues. Acupuncturists, chiropractors, midwives, homeopaths, naturopaths, reflexologists, registered massage therapists, and other complementary medicine practitioners may also collect, use and disclose personal health information.

From private practitioners' offices, some personal health information may go to pharmacies, medical laboratories, medical imaging centres, insurance companies, accreditation bodies and public or private insurance plans. If an individual uses an employer-based health, extended health or dental insurance plan, or employer-based health services, some of his or her personal health information may proceed back to the employer. It can also be disclosed for research purposes by physicians and hospitals to private sector research organizations. These are some of the routes personal health information can take as it is used for primary purposes in patient treatment, and secondary purposes in health care provider disbursement or review, epidemiological research and hospital and health system analyses.

In the health sector, public and private distinctions are difficult to discern, largely because the public and private health sectors work together to foster individual patient and population health. In British Columbia, most health care bodies are subject to the privacy protection measures contained in British Columbia's public sector privacy legislation, the *Freedom of Information and Protection of Privacy Act*, including hospitals and agencies contracted by hospitals, the Medical Services Plan, Pharmanet and the Ministry of Health. BC's universities, some of which conduct health research, are also covered by the public sector legislation. Health care professionals have a duty of confidentiality according to professional codes of conduct, which are enforced through professional governing bodies. Legislation like the BC *Health Professions Act* also strengthens the confidentiality obligation of health care professionals.[77] However, there is no privacy legislation governing the private health care sector, which includes doctors' offices, dentists, complementary medicine practitioners, medical labs, pharmacies, and health research organizations.

There are numerous pressures to create parity between the public and private health care sectors with regard to the privacy protection of personal health information. Different privacy requirements for public and private health care professionals and organizations mean that patients are not guaranteed the same privacy standards across the health care continuum. Consistency between the public and private health sectors would also help to simplify privacy rules for health care actors and institutions, protect individuals against potential privacy threats arising from developments in telehealth and expansive health research initiatives.

The complexity of public-private linkages in the health sector and the lack of consistency with regard to the current privacy law context can create confusion in the application of legislated privacy requirements to health information. For example, when doctors or dentists deliver patient care in a hospital, the patient information that results is considered the property of the hospital, and the public sector law applies. When a doctor or dentist in his or her private office delivers treatment, the resulting information is not protected by the BC *Freedom of Information and Protection of Privacy Act*. Some private physicians' offices are located in hospitals, which can complicate things further. Some private sector research organizations can obtain health information from hospitals, and some hospitals are joined with university centres for medical teaching and research. The mix of public and private sector activity in health care settings means that it is sometimes difficult to distinguish between information held by public or private sector agencies.

In recent years, federal and provincial governments throughout Canada have undertaken telehealth initiatives that have made the consistent privacy protection of personal health information more urgent. The federal telehealth strategy centres on the Canada Health Infoway. The Infoway is a "health information highway", a network that will link federal, provincial, regional and non-governmental health information sources into a single storage, access and retrieval system. The Infoway is expected to enable health care providers, caregivers, patients, the public, administrators, policymakers and researchers to access, share and create health information on topics ranging from current healthy lifestyles and policies, to research on diagnoses and treatment, and empirical cost and efficiency indicators.

One "key link in the information chain" of the Canada Health Infoway is a system of electronic health records."[78] Electronic health records will

> *promote safe, rapid, effective treatment for patients by allowing health care professionals, anywhere in Canada, access to patients' health records and personal medical histories..., 24 hours a day, seven days a week. This will reduce the likelihood of misdiagnoses, unnecessary and sometimes risky tests and x-rays, and expensive duplicate tests that might be undertaken if a patient's full medical history were not available.*"[79]

British Columbia's Ministry of Health has initiated a similar plan for health information management in the province. British Columbia's telehealth plan is being designed to integrate health system information and benefit the BC health system by,

- *enabling British Columbia residents, physicians, nurses and other health service providers access to specialists hundreds of kilometers away;*
- *providing timely access to patient/client data thereby reducing unnecessary duplication of tests and improving quality of care;*
- *reducing the need for patient travel/transfer and physician travel by transmitting data and diagnostic quality images instead of people;*
- *improving links between physicians, nurses, hospitals, pharmacies and other health providers in a cost-efficient manner;*
- *creating efficiencies and savings that will offset capital and operating costs.*"[80]

According to the Ministry of Health, the "integrated health record" - a patient-centred, comprehensive medical record - is central to this program of service integration. BC's telehealth program therefore includes a plan to develop an integrated health record for each health care user in British Columbia. The record will be a compilation of each individual's personal health information, gathered from all parts of the health sector, into a register of "an individual's lifetime health status and health services."[81]

The use of information technologies in the health sectors has improved, and is expected to further enhance, timely diagnosis and treatment, information accuracy and availability, and cost savings. Computerized hospital records have many benefits over paper systems: "[p]aper files can be read by only one person at one time, and they are unavailable nearly 50 percent of the time (e.g. in another doctor's office or misfiled)."[82] Networked or CD-ROM databases of medical journal articles and books allow health professionals to access complete and up-to-date information on diagnoses and treatment more readily than when libraries were the only source of these kinds of materials. There are also databases that can help medical professionals to diagnose illness by entering symptoms as search terms. Telemedicine is particularly useful for health care providers and hospitals outside of major urban centres. Professionals can consult more easily with colleagues in other cities or countries, with all parties simultaneously viewing a real-time patient examination, a medical image or test results. Computerized records also make it easier to undertake statistical research on diseases and treatments. Access to this kind of information has demonstrated benefits to effective patient care and lower health system costs.

These electronic health initiatives are not a distant goal. As one individual told the Committee, "we are in the age of the distributed electronic patient record. It is not something futuristic.. Health Canada has engaged in a process of networking all health care institutions, and they are currently thinking in terms of five to ten years to accomplish this."[83]

Health care practitioners, administrators and researchers want consistent privacy protection measures built in at the outset of telehealth development, believing that the privacy of health information is essential, but also that privacy issues have the potential to impede the progress of electronic health networks. The electronic linkage of personal information and health system data will require consistency in many different respects; technological formats, data formats, and privacy rules will have to be standardized. The International Medical Informatics Association has begun to develop and recommended policies for a health information privacy policy that can be adopted uniformly around the world. Likewise, Health Canada is coordinating the development of a "health information privacy harmonization plan" with the Protection of Personal Health Information Working Group.

The diverse interests that meet in discussions concerning the privacy protection of personal health information make this area one of the most difficult from a privacy perspective. In this area, the need to consider conflicting fundamental values comes into sharp focus: the need to allow health care providers, health system administrators and health researchers to use health information in a way that can benefit the health system and therefore society as a whole, and the need to guarantee the privacy rights of individuals. Media reports tell us that we should fear for the integrity of Canada's universal public health system due to escalating health care costs and funding crises. Some witnesses indicated that the scientific analyses provided by commercial health research firms are vital to the cost effectiveness, and consequently, the well-being of the public health care system. Accordingly, some witnesses urged the Committee to recognize the need for harmonized privacy laws across multiple jurisdictions that balances health researchers' requirement for personal health information with individuals' rights to personal privacy:

> *As a matter of public policy and ethical theory, it is unhelpful to argue whether a system of health information that benefits society as a whole is more important than a person's right to privacy or vice versa. A social contract that reasonably balances the value of both is necessary for the ultimate benefit of the individual in society.*[85]

BC's Information and Privacy Commissioner also advised the Committee that initiatives towards electronic patient records and the "health information highway" must balance privacy and health system interests: "the possibility of cost savings and the push to be pragmatic should not be the sole driver of what's being done in this area. The idea that privacy should very much be factored in at the outset of project design and policy formulation is, I think, very broadly shared across a wide spectrum."[86]

76 percent of British Columbians said it is very important that medical or health information must be kept private.[83]

61 percent of British Columbians "trust completely" that individual health care professionals, such as doctors, dentists, massage therapists, and so on, will be careful with information they might have about individuals.

53 percent trust hospitals completely;

52 percent trust pharmacies completely; and

48 percent trust medical laboratories completely with their personal health information.[84]

Numerous observers have noted the failure of information societies to progress with ethical guidelines at a pace that matches developments in technology and science. Advances in genetics have attracted a great deal of criticism in that respect. As one witness explained, genetic information,

- *relates to health, to quality of life, and to the sense of fairness in the lottery of birth and treatment of the disadvantaged.*
- *relates to race, ethnicity, and parentage.*
- *relates to gender (and maybe to sexuality).*
- *has relevance for mental competencies and tendencies, and to behavioral predisposition.*

Health care practitioners, administrators and researchers want consistent privacy protection measures built in at the outset of telehealth development, believing that the privacy of health information is essential, but also that privacy issues have the potential to impede the progress of electronic health networks. The electronic linkage of personal information and health system data will require consistency in many different respects; technological formats, data formats, and privacy rules will have to be standardized. The International Medical Informatics Association has begun to develop and recommended policies for a health information privacy policy that can be adopted uniformly around the world. Likewise, Health Canada is coordinating the development of a "health information privacy harmonization plan" with the Protection of Personal Health Information Working Group.

The diverse interests that meet in discussions concerning the privacy protection of personal health information make this area one of the most difficult from a privacy perspective. In this area, the need to consider conflicting fundamental values comes into sharp focus: the need to allow health care providers, health system administrators and health researchers to use health information in a way that can benefit the health system and therefore society as a whole, and the need to guarantee the privacy rights of individuals. Media reports tell us that we should fear for the integrity of Canada's universal public health system due to escalating health care costs and funding crises. Some witnesses indicated that the scientific analyses provided by commercial health research firms are vital to the cost effectiveness, and consequently, the well-being of the public health care system. Accordingly, some witnesses urged the Committee to recognize the need for harmonized privacy laws across multiple jurisdictions that balances health researchers' requirement for personal health information with individuals' rights to personal privacy:

> *As a matter of public policy and ethical theory, it is unhelpful to argue whether a system of health information that benefits society as a whole is more important than a person's right to privacy or vice versa. A social contract that reasonably balances the value of both is necessary for the ultimate benefit of the individual in society.*"[85]

BC's Information and Privacy Commissioner also advised the Committee that initiatives towards electronic patient records and the "health information highway" must balance privacy and health system interests: "the possibility of cost savings and the push to be pragmatic should not be the sole driver of what's being done in this area. The idea that privacy should very much be factored in at the outset of project design and policy formulation is, I think, very broadly shared across a wide spectrum."[86]

76 percent of British Columbians said it is very important that medical or health information must be kept private."[84]

61 percent of British Columbians "trust completely" that individual health care professionals, such as doctors, dentists, massage therapists, and so on, will be careful with information they might have about individuals.

53 percent trust hospitals completely;

52 percent trust pharmacies completely; and

48 percent trust medical laboratories completely with their personal health information."[84]

Numerous observers have noted the failure of information societies to progress with ethical guidelines at a pace that matches developments in technology and science. Advances in genetics have attracted a great deal of criticism in that respect. As one witness explained, genetic information,

- *relates to health, to quality of life, and to the sense of fairness in the lottery of birth and treatment of the disadvantaged.*
- *relates to race, ethnicity, and parentage.*
- *relates to gender (and maybe to sexuality).*
- *has relevance for mental competencies and tendencies, and to behavioral predisposition.*

- *has relevance for descendants, and therefore possibly to reproductive choices.*[87]

Genetic information also opens the possibility of increased stigmatization and discrimination on the basis of any of those factors. It is therefore expected that in time, advances in genetic research will compel society at large to engage in ethical and social policy discussions that are beginning now with the issue of information privacy around questions such as definitions, ownership and legitimate uses of personal information.

Individuals and organizations that addressed the Committee agreed that personal health information is a sensitive form of personal information that requires sound privacy protection. The Committee also heard that health care professionals have earned the trust of British Columbians: they believe strongly that medical or health information must be kept private, but a large majority also reported that they have a high level of trust for those in the health sector to whom they provide their personal information.

For their part, health care providers in the private sector indicated that they are very sensitive to individuals' privacy concerns:

> *Doctors and dentists are very sensitive to privacy concerns and have adjusted their practices to be more considerate of this issue. The information they collect is generally used in treating the patient directly; however, medical practitioners may contribute patient information to research studies. They are adamant, however, in the gaining patient permission before any confidential information is shared.*
>
> *While those in the medical and dental professions gather the most private of information from their patients, their security measures do not seem to measure up. Individual files are stored in filing cabinets (usually in a common area) within the office, which is locked and alarmed.*
>
> *These professionals however, are concerned about the transference of patient information electronically. There is some support for the argument that there are cost savings in this process as they do see the potential benefits of using information technology to stretch health care dollars. However, the protection of privacy is the bigger priority. The more technology is used in administering health care, the more difficult it is to protect privacy of patients. Health care professionals know that there are many parties interested in individual patients' health care information, including employers and insurance companies.*
>
> *The counselor interviewed in this study reported a very conservative approach regarding patient records and who is entitled to have access to them.... [N]o clerical staff had access to his files (he himself filled out any and all forms with contact information, etc). Furthermore, the patient has complete control over the information kept on file and he would not release it, even if the patient had switched to another counselor, without the patient's express, written consent. He had never offered patient information as part of a research initiative, but said that for this also, the ethics of his profession would oblige him to get patient permission beforehand.*[88]

Conversely, one witness told the Committee:

> *I am a medical doctor by basic training, and I have worked in the health information field for 30 years. I am personally of the opinion that the medical profession is not the appropriate guardian for privacy, because my experience is that medical professionals believe that they do guard privacy.... We all feel committed to the Hippocratic oath, and we all feel committed to guarding the privacy of patients. But it's a fallacy.*[89]

This witness explained that privacy threats to health information systems largely come from authorized professionals through negligent or inappropriate use.[90] With respect to personal health information held by private physicians, another witness told the Committee, "I have had major difficulty in having to follow up and correct factual errors that are in these private records. At one point I finally thought: that's not my job."[91] For other individuals, concern about health information privacy centres on networked health databases and the contracting-out of health information management.

INFORMATION PRIVACY RIGHTS

While privacy protection has come into social policy arenas at different times during the twentieth century, the twenty-year transformation in information technologies has now resulted in a heightened public concern about information privacy in private sector transactions. Information privacy focuses on the protection of the privacy of personal information, or personal data, which has been defined as "information about an identifiable individual that is recorded in any form, be it electronically or on paper."[92] In general, personal information is recorded information that is about a particular, recognizable person.

Privacy experts have attempted to define privacy in various ways:

> *"The extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention." (Ruth Gavison)*
>
> *"A degree of inaccessibility of persons, of their mental states, and of information about them to the sense and surveillance devices of others." (Anita Allen)*
>
> *"the 'claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others.' In other words, privacy would be 'the right to exercise some measure of control over information about oneself.'"*[93]

While privacy is a concept that is difficult to put into words, the experience of privacy itself, and the lack of it, is easily understood. The word privacy may evoke an array of impressions: self-determination, freedom, autonomy, dignity, individuality, familiarity, intimacy, sanctuary, solitude, or introspection.

Privacy is a necessary state in human societies. It is one of the elements that enables individuals to self-actualize:

> *Privacy…allows us to shed our public roles from time to time. We cannot be "on" all the time. Periodically, we need "time out" just to be ourselves: irritable, cranky, angry, or self-indulgent, to escape to the anonymity of a park or city street or a bar, among strangers.*
>
> *Sometimes we need to experiment with new ways of doing things, to make serious or silly adjustments to the rituals of our lives, without the shame or embarrassment that the exposure of most of these efforts would cause.*
>
> *Finally, we sometimes just need to be completely alone.*[94]

The freedom to develop as unique personalities within a community is one reason that democratic societies preserve human rights and freedoms. Violations of privacy, which reveal an individual's personal thoughts, qualities or behaviour to unauthorized persons, are often related to the estimation of an individual relative to informal norms. Violations of privacy can expose the individual to judgement, criticism, and prejudice because the qualities of his or her private life do not match the views held by others. Human rights, which guarantee "the accommodation of differences,"[95] recognize the idea that individuals need a degree of protection from social conformity beyond the social norms expressed by the law.

Privacy also helps individuals to exercise their rights and freedoms. For example,

> *The right to free assembly can be chilled or damaged by excessive knowledge about you, say through video surveillance. If you know that there are going to be cameras picking you out as an individual, depriving you of your anonymity, that might reduce your inclination to assembly, or indeed, your inclination toward free speech.*[96]

The BC Human Rights Commission has also recognized the importance of information privacy. The Commission has recommended that the *BC Human Rights Code* be amended to "[p]rohibit any request by employers for information from a job applicant about a prohibited ground of discrimination" because it simply leaves job applicants open to discrimination.[97]

Information privacy, or data protection, the term used commonly in Europe, achieved legal recognition in many nations during the 1980s, as governments increased their use of mainframe computers. It was understood that the capabilities of computer databanks had increased potential threats to individual privacy over and above concerns inherent to even paper-based records systems, and governments wanted to ensure that the needs of the public sector for personal information to administer programs and to maintain accountability could be balanced with the right to privacy.

With the rapid development of integrated computer and communications technologies, concerns about information privacy shifted in the 1990s to a much wider expanse. Cheaper, smaller, and now common technologies that can collect, manipulate, store and transmit data in all electronic formats are now used routinely in the private sector for a whole range of business activities. The diffusion of privacy concerns into the private sector has given rise to a new privacy discourse; one based more on consumer rights than on human rights.[98]

Traditionally, individuals are thought to have a great degree of choice in their interactions with businesses and other private sector organizations. In theory, the marketplace allows individuals to choose from a range of products and services offered by various businesses and organizations. They can choose not to purchase a particular product or service, or choose not to deal with a particular business or organization whose business practices they consider unacceptable. However, with consumer protection measures relating to product safety, fair trade, product quality and dispute resolution,[99] governments have acknowledged that in the marketplace, consumers are disadvantaged relative to businesses since there are "asymmetries of information, preferences and bargaining power between businesses and consumers."[100]

Information privacy initiatives also recognize that individuals have unequal bargaining power in their relationships with private sector businesses and organizations,[101] particularly regarding

- an understanding of business practices and the uses to which their personal information may be put
- the amount of time and energy individuals would have to spend to obtain all of this information about every organization with whom they do business
- the power to refuse to disclose information when it is requested
- the power to challenge any unfair information practices engaged in by a particular business or a business sector

As a result of the unequal position of individuals versus private sector businesses and organizations, individuals may be compelled to give up more of their informational privacy than they would like to, or to give up more than they realize, in exchange for the products and services they want to purchase.

Some privacy advocates have outlined compensation frameworks based on the notion that in commercial transactions, consumers' personal information is a commodity exchanged for business goods or services and should be accounted for as such. For example, one such proposal is to establish a legislated property right that would require individuals to consent to the commercial use of their personal information, with consumer "royalties" collected from businesses and paid to individual consumers through a specially created agency.[102]

However, there is some agreement among privacy experts that in private sector transactions, granting the *control* over personal information to the subject of that information represents a convergence between human rights-based and consumer rights-based approaches to information privacy.[103] By giving individuals control over their personal information, individuals are free to decide what information they are willing to provide in private sector transactions, and under what terms. Around information privacy, the internationally accepted framework for restoring consumers' bargaining power are the fair information principles. Fair information principles provide individuals with the means to control the collection, use, and disclosure of their personal information.

FAIR INFORMATION PRINCIPLES

Information privacy or data protection legislation emerged in many European jurisdictions in the 1980s as a way of providing individuals with information privacy rights in their private sector transactions, but it was also recognized that uniformity in privacy protection regimes was needed to simplify the rules for business and to facilitate international trade.

The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* aimed to harmonize data protection regimes among trading partners by setting out widely accepted minimum standards for the use of personal data and influencing member states to adopt them so that the flow of information across national boundaries would not be obstructed to the detriment of business. As a number of states and supra-national bodies implemented legal instruments based on such initiatives, their principles converged into a list of universally-recognized data protection standards called "fair information principles."[104]

The European Union's 1998 *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data* is the most recent and strongest international expression of the fair information principles originally articulated in the OECD Guidelines. The Directive professes to ensure that citizens of all EU member states willl receive equal protection of their personal information, and that the free flow of information will not be obstructed by dissimilar privacy laws. In contrast to earlier data protection instruments like the OECD Guidelines, the EU Directive is binding on the Union's member states. It declares that EU member states must pass legislation to the effect that the transfer of personal data to a third country may take place only if "the third country in question ensures an adequate level of protection."[105]

While this extra-territorial requirement has offended some governments' sense of sovereignty, most have nonetheless agreed that consensus on fair information principles and cooperation with the EU Directive will protect the interests of individual consumers, facilitate business processes, and allow for unimpeded growth of the new economy. Even the United States government, which stridently opposed the extraterritorial reach of the EU Directive, came to an agreement with the European Union, after three years of negotiations, on a self-regulatory regime for American companies that meets the EU Directive's requirement for adequate data protection standards. This standard, the "safe harbor" framework, is also based on the internationally-recognized fair information principles.

In Canada during 1990s, The Canadian Standards Association, business, consumers and government worked together to develop a voluntary Canadian privacy standard based on the fair information principles. The result was the 1996 Canadian Standards Association Model Code for the Protection of Personal Information. At the same time, privacy advocates, government officials and e-commerce interests were investigating the possibility of a federal privacy law of general application for the private sector. Because the CSA Model Code was designed with input from all economic sectors in Canada, it expresses the fair information principles in a manner that reconciles Canadian business interests with the international standards for privacy protection. Therefore, many agreed with Industry Canada's view that,

> *[s]ince the same basic set of fair information practices is found in legislation throughout the world, any of these could serve as the basis of the law. It would make sense, however, to build on the consensus that has been achieved around our National Standard. The CSA Standard has been acknowledged in many forums as an improvement over the OECD Guidelines. Principles based on the CSA Standard would help to ensure compatibility with other regimes that have also legislated to a higher standard than the Guidelines, such as Quebec.*[106]

The federal *Personal Information Protection and Electronic Documents Act* received Royal Assent in April 2000. That legislation incorporates and gives the force of law to the CSA Model Code's ten fair information principles: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

ACCOUNTABILITY

The accountability principle requires that an organization take responsibility for the personal information it collects, uses, discloses and retains.

To promote adherence to this principle, the CSA Model Code states that "an organization is responsible for personal information under its control" and requires that an organization designate and identify an individual or individuals to oversee the organization's compliance with fair information principles. The individual(s) designated should oversee the information practices of the organization, including information transfers, and respond to inquires and complaints.

IDENTIFICATION OF PURPOSES

The identification of purposes principle requires organizations to notify consumers about how they intend to use personal information so that consumers can make informed decisions about the information they consent to provide in private sector transactions. The Canadian Standards Association advises that the identification of purposes principle requires that any anticipated or possible subsequent or secondary uses of personal information should be identified, and an individual given the option of accepting or rejecting those uses.[107]

The identification of purposes principle also reminds organizations to collect only the information that they need for legitimate business uses. As explained by the Canadian Information Processing Society,

> *[i]dentifying purposes for the personal information which is to be collected allows organizations to focus their data collection on only that information which is necessary for the stated purposes, or to find alternatives to the collection of personal information. This is critical to effectively limiting collection (principle 4). This should not be viewed as a constraint on the organization. Since data collection and maintenance is expensive, "identifying purposes" is the first step in reducing operating costs.* "[108]

To meet this principle, the CSA Model Code requires organizations to "clearly define and document" the purposes for which information will be used before they collect information. The federal *Personal Information Protection and Electronic Documents Act* incorporates the principle as stated above, and in section 5(3) adds the requirement that an organization may only collect, use and disclose personal information for purposes "that a reasonable person would consider appropriate in the circumstances."

CONSENT

The principle of consent is the core of the fair information principles. Consent requires that an individual be able to decide when, to whom and for what purposes any of their personal information will be collected, used, disclosed or retained. Discussions surrounding the meaning of consent generally focus on how to ensure that consent is informed and voluntary, and how to determine that consent has been given. The central terms in these discussions are express consent, implied consent, informed consent, and coerced consent.

Express consent is the most reliable expression of consent. It is therefore especially important for sensitive personal information. Express consent is given when an individual explicitly authorizes the collection, use or disclosure of his or her personal information, whether by verbal agreement, or by signing a form, checking off a consent box, or completing a computerized form.[109]

Implied consent is consent that is presumed by the actions of the data subject. For example, when using a credit card to make a purchase, it is assumed by the merchant and the credit grantor that a consumer's credit card number can be used for billing by the fact that he or she provided the card. Implied consent is also the form of consent given when a business or organization offers a negative option, such as a check-off box to refuse consent for information sharing.

It is well-established that consent should be given with adequate information about the effects that the consent may have; for example, an individual should know, before giving consent, "what information will be collected, who will have access to it, how it will be used, and to whom it may be disclosed.[110] The CSA Model Code states that "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."[111] Inappropriate circumstances are normally those in which obtaining consent will undermine the purpose for obtaining the information, such as investigations, or when the information collection, use or disclosure is clearly in the interests of the data subject and consent cannot be obtained, such as a medical emergency.

Coerced consent occurs when a business or organization uses undue influence in order to obtain consent.[112] It has been suggested that undue influence on consent is likely to exist "where the consent of an individual to the collection, use or disclosure of secondary or extraneous information has been obtained as a condition of providing a product or service over which the organization has exclusive control."[113] The Canadian Standards Association also explains that "requiring consent to secondary or extraneous information uses as a condition of supplying a product or service... is inconsistent with the CSA Model Code. Whenever consent is provided, it must be provided freely and willingly."[114]

One organization urged the Committee to carefully consider the definitions of "implied consent" and "consistent purposes". These terms can allow data controllers to circumvent the basic principles of privacy protection. For example, implied consent is reasonable when a pharmacist needs information from a physician to fill a prescription, but should a patient's implied consent in entering into a physician's care also be understood as consent to use patient information for secondary research purposes?"[115] Is secondary research a purpose consistent with medical treatment? It was also suggested that exemptions to notice and opt-out requirements would significantly weaken the privacy protection provided by the consent requirement.

LIMITING COLLECTION

This principle requires that organizations collect "only the data necessary and relevant to the specified purposes" and that organizations collect personal information "by fair and lawful means."[116]

The principle of limiting collection is closely related to the identifying purposes principle and the principle of consent. It is intended to reduce the possibility of information being collected through coercive or deceptive means, of inappropriate disclosures and use of personal information for purposes that were unintended at the time of collection.

LIMITED USE, DISCLOSURE AND RETENTION

This principle states that

> *"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes."*[117]

Closely related to the limiting collection, consent, and individual access principles, the principle of limited use, disclosure and retention is designed to ensure that personal information that has been collected by an organization is only disclosed to authorized personnel and only for fulfilling business purposes, and that disclosures unrelated to the original and approved business purpose do not take place without the consent of the data subject.

Conformity to this principle would preclude the sale or trading of databases of personalized consumer information after the information had fulfilled its original transactional purpose unless consumers had been notified of this secondary use prior to the collection of their personal information, and consented to it. It would also prevent an organization from retaining personal information used to complete a specific transaction in order to use it for future, as yet undetermined purposes.

> *Once the requirements of the original purpose have been met, if an individual has not consented to any further information use, the personal information should be destroyed, erased or made anonymous. For example, if an individual completes an application form but subsequently decides not to sign the authorization, any data collected from the individual should not be retained unless the individual consents to other uses.*
>
> *However, where an individual applies for, but does not qualify for services, the organization must retain the information for a reasonable length of time in case of a challenge.*
>
> *Organizations should develop guidelines and procedures with respect to retention, including minimum and maximum retention periods.'*[118]

ACCURACY

This principle states that "personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[119] As the Canadian Standards Association explains, this principle is meant to "prevent individuals from being unfairly discriminated against or harmed by inaccurate or inappropriate information":

> *Privacy surveys conducted in Canada indicate that Canadians are extremely concerned about the prospect that inaccurate and inappropriate information may be used to make decisions that will affect them. This is particularly a concern when dealing with such sensitive information as employment records or health or financial that that, if erroneous, may unfairly limit their opportunities to find employment, obtain credit, or acquire services, or which may in other ways damage their reputation or standing within the community.*[120]

The identifying purposes and limiting collection principles support this one, since when extraneous information is collected, there is a greater likelihood of collecting information that is inadequate to unanticipated secondary purposes, and the more information collected, the greater chance there is of collecting inaccurate information.

SAFEGUARDS (SECURITY)

This principles requires organizations to protect personal information "by security safeguards appropriate to the sensitivity of the information."[121]

In recognition that accidental disclosures or unlawful access to personal information are a serious threat to information privacy, this principle requires organizations to protect all forms of personal information, throughout its life cycle, against "loss or theft, as well as unauthorized access, disclosure, copying, use or modification" by training personnel in appropriate security procedures and by using "a range of physical, organizational, and technological measures."[122]

OPENNESS

The CSA Model Code expresses the principle of openness as follows: "[a]n organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."[123]

This principle requires that organizations ensure that the public and its employees can obtain meaningful information about the personal information they collect, use and disclose; how its information handling practices are managed to comply with the fair information principles; procedures for accessing or correcting personal information; and procedures for lodging complaints. The Canadian Standards Association explains that this principle is meant to ensure that "individuals can reasonably act on information protection principles adopted by the organization."[124].

INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[125]

The individual access principle requires organizations to maintain personal records in such a way as to facilitate individual access at no cost or at a reasonable cost to the data subject, and to ensure that the identify of individuals seeking access are verified. The Canadian Standards Association explains that under this principle, files that are provided the to data subject "should provide a comprehensive picture of what information is maintained, its source, how it is used, and any other pertinent details of collection, use disclosure, retention or disposal. All of these details should have been documented in complying with Principle 2, Identifying Purposes."[126]

MECHANISMS FOR CHALLENGING COMPLIANCE

"An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."[127]

This principle is designed to provide individuals, whether customers, clients or employees, with an avenue for verifying an organization's compliance with the fair information principles. To that end, this principle requires that organizations identify a contact person or department and a procedure for receiving and handling complaints.

PART 2 – INFORMATION PRIVACY RULES FOR BRITISH COLUMBIA'S PRIVATE SECTOR

LEGISLATION

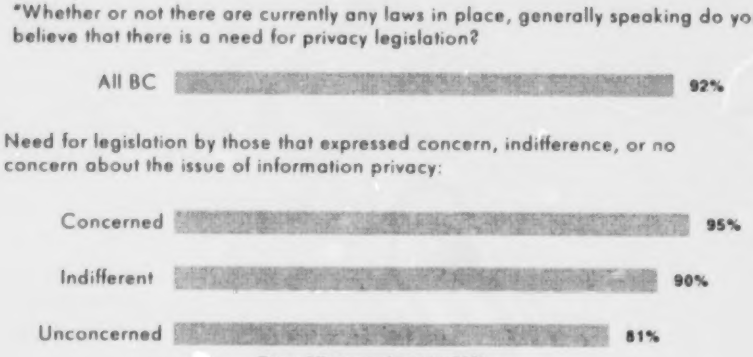
Recommendation 1:

The Committee recommends that the government of British Columbia enact legislation to protect the information privacy of personal information held in the private sector, and that the proposed legislation achieve a fair and workable balance between information privacy and the use of personal information for legitimate private sector purposes.

Most individuals, businesses and organizations expressed the view that British Columbia should pass privacy legislation to regulate the collection, use, disclosure and retention of personal information by the private sector. As one individual wrote,

> *I have become very concerned about the amount and nature of personal information that is being collected on individuals. As the name implies it is personal information, yet in this age of machines that know no boundaries, it has become very easy to exchange information at the click of a mouse button. What protection is there for the individual? Very little. And as the federal government rushes ahead with its plan to wire all of Canada to the Internet, more of our personal information becomes accessible to others.*[128]

Ipsos-Reid also reported that a full 92 percent of survey respondents said that they believe there is a need for privacy legislation for the private sector.



Need for Legislation

Base: All respondents (n=600)

Individuals, businesses and organizations gave several reasons for supporting legislated information privacy protection for the private sector. In addition to the privacy concerns already discussed, individuals and organizations suggested that privacy legislation might benefit the private sector.

Some of the benefits that private sector businesses and organizations should expect are clarity of the rules, a "level playing field", and increased consumer confidence. For example, one organization told the Committee that it supports regulation because it will likely enhance public confidence in the marketing research industry, especially since it will bring disreputable market researchers into line with the fair information principles.[130] Another organization recognizes that fair information practices are necessary for the insurance industry, given that the industry depends on the use of personal information, is very competitive, and is one that requires consumer confidence in order to thrive.[131]

When asked, "Do you agree or disagree with the statement: "Privacy legislation will help businesses in the long run, because consumers will trust them more", 52 percent of British Columbians said they agree, and 8 percent said they disagree.[129]

The Committee also heard that the success of Canada's e-commerce sector - particularly Internet-retailing - depends upon building consumer trust by providing reasonable protection of personal information and privacy. Canada's e-commerce development is lagging due to a lack of consumer confidence in the privacy and security of Internet transactions. Some businesses told the Committee that a regulatory framework for private sector privacy is required to enhance consumer confidence and allow Canada's e-commerce sector to keep pace with other jurisdictions.[132]

The fairly low levels of trust British Columbians report for financial, retail and Internet businesses indicate that businesses are probably correct in assuming that privacy legislation for the private sector would enhance business competitiveness by improving consumer confidence. In fact, most British Columbians also agreed that "privacy legislation will help businesses in the long run, because consumers will trust them more":

> *When it comes to the potential impact of information privacy legislation, British Columbians tend to be quite optimistic. Most agree that businesses will be helped by this kind of legislation, in that consumers will trust them more (52% strongly agree, just 8% strongly disagree). Very few believe that legislation will create red tape that will hurt the economy (just 14% strongly agree while 41% strongly disagree). Further, this optimism may be behind the widely held opinion that it is more important to protect consumers than to make things easier for business (73% strongly agree).*[133]

However, private sector businesses and organizations also voiced concerns that privacy legislation could have a negative effect, especially due to the possible increase in red tape and costs to business of implementing and maintaining the privacy provisions required by the legislation, but also because they speculate that some business practices may not be allowed under a new privacy law. Some businesses are also concerned that in time, as more consumers exercise their right to opt-out of information collection and circulation processes, there will be less data available for exchange, whether for advertising, the management of operational risks, or administrative purposes. One business representative explained that for the efficient administration of customer business, customer information must be shared with affiliates and third parties contracted to provide administrative services, such as loan collections and the printing of cheques.

In fact, most British Columbians emphasized that provincial privacy legislation must strike a workable balance between the needs of businesses and the rights of consumers. One individual also told the Committee, "[t]he questions raised about whether or not this would isolate BC or hurt the economy... . It is something to be looked at very carefully and clearly. It wouldn't do to have an ideal law which resulted in business locating in Alberta."[134] Another organization offered a compelling opinion, stating that just as "[i]ntegrity in personal information collection systems is a social good; so too is an efficient market... ."[135] One business representative gave this notion a stronger expression:

> *We have to support capitalism in our country... People need to understand that businesses have to advertise. Everyone's so worried about individual rights that they are forgetting about society as a whole, forgetting about the whole system... They are a part of that system, and they have to partake in it. They should not be able to opt out for free, because they are opting out of a system that makes money.*[137]

Most British Columbians do believe that the interests of both consumers and businesses must be considered, but ultimately, they believe that consumers' privacy must be the primary objective of any proposed legislation. As one individual explained,

> *[w]hatever* [privacy protection] *solution B.C. proposes..., it is important to bear in mind that privacy legislation is intended to protect individuals from abuses by those who provide goods and services. The European Directive and other data protection legislation distinguish between data subjects and data controllers. The former are given the rights; the latter the responsibilities. Governments, businesses and professionals are data controllers. It is very important to keep this distinction in mind.*[139]

When asked "Do you agree or disagree with the statement: Privacy legislation will just create more red tape for businesses, and that's bad for the economy", 14 percent of British Columbians said they strongly agree, and 41 percent of British Columbians said they strongly disagree.[136]

SELF-REGULATION

Some witnesses to the Committee favour a self-regulatory approach, rather than provincial privacy legislation. For example, one organization wrote that, " a self-regulatory approach is preferable to governmental regulation, since the former provides more flexibility for both industry and regulators and requires fewer public resources to implement."[140] As mentioned, a number of larger businesses and industry associations are also experienced in developing and using their own privacy codes.

> *The Committee heard, however, that for the most part, British Columbians are not convinced that private sector businesses and organizations will adequately manage the privacy of their personal information in the absence of legislation: Overall, legislation was seen as the only viable way to protect information privacy. Although a few participants noted that "it would be nice" if private sector organizations could self-regulate their handling of personal information, participants felt it is simply not realistic to expect all companies to regulate themselves. As long as compliance with basic principles is voluntary, some companies will choose not to follow them.*[141]

When asked, "Do you agree of disagree with the statement: It's more important to protect consumers than to make things easier for business", 77 percent of those who are concerned about information privacy said they strongly agree, and 60 percent of those who said they are not concerned about the issue also agreed with that statement.[138]

Those views are supported by the levels of trust British Columbians indicated for private sector enterprises. Ipsos-Reid asked respondents to rate how much they trust different kinds of private sector organizations to "be careful with information they might have about individuals," and reported the following:

> *approximately one-third say they have a great deal of trust that banks (36%) and credit unions (34%) will be careful with information they may have about them....*

Some of the benefits that private sector businesses and organizations should expect are clarity of the rules, a "level playing field", and increased consumer confidence. For example, one organization told the Committee that it supports regulation because it will likely enhance public confidence in the marketing research industry, especially since it will bring disreputable market researchers into line with the fair information principles.[130] Another organization recognizes that fair information practices are necessary for the insurance industry, given that the industry depends on the use of personal information, is very competitive, and is one that requires consumer confidence in order to thrive.[131]

> ***When asked, "Do you agree or disagree with the statement: "Privacy legislation will help businesses in the long run, because consumers will trust them more", 52 percent of British Columbians said they agree, and 8 percent said they disagree."[129]***

The Committee also heard that the success of Canada's e-commerce sector - particularly Internet-retailing - depends upon building consumer trust by providing reasonable protection of personal information and privacy. Canada's e-commerce development is lagging due to a lack of consumer confidence in the privacy and security of Internet transactions. Some businesses told the Committee that a regulatory framework for private sector privacy is required to enhance consumer confidence and allow Canada's e-commerce sector to keep pace with other jurisdictions.[132]

The fairly low levels of trust British Columbians report for financial, retail and Internet businesses indicate that businesses are probably correct in assuming that privacy legislation for the private sector would enhance business competitiveness by improving consumer confidence. In fact, most British Columbians also agreed that "privacy legislation will help businesses in the long run, because consumers will trust them more":

> *When it comes to the potential impact of information privacy legislation, British Columbians tend to be quite optimistic. Most agree that businesses will be helped by this kind of legislation, in that consumers will trust them more (52% strongly agree, just 8% strongly disagree). Very few believe that legislation will create red tape that will hurt the economy (just 14% strongly agree while 41% strongly disagree). Further, this optimism may be behind the widely held opinion that it is more important to protect consumers than to make things easier for business (73% strongly agree).*[133]

However, private sector businesses and organizations also voiced concerns that privacy legislation could have a negative effect, especially due to the possible increase in red tape and costs to business of implementing and maintaining the privacy provisions required by the legislation, but also because they speculate that some business practices may not be allowed under a new privacy law. Some businesses are also concerned that in time, as more consumers exercise their right to opt-out of information collection and circulation processes, there will be less data available for exchange, whether for advertising, the management of operational risks, or administrative purposes. One business representative explained that for the efficient administration of customer business, customer information must be shared with affiliates and third parties contracted to provide administrative services, such as loan collections and the printing of cheques.

In fact, most British Columbians emphasized that provincial privacy legislation must strike a workable balance between the needs of businesses and the rights of consumers. One individual also told the Committee, "[t]he questions raised about whether or not this would isolate BC or hurt the economy. . . It is something to be looked at very carefully and clearly. It wouldn't do to have an ideal law which resulted in business locating in Alberta."[134] Another organization offered a compelling opinion, stating that just as "[i]ntegrity in personal information collection systems is a social good; so too is an efficient market. . . ."[135] One business representative gave this notion a stronger expression:

> *We have to support capitalism in our country... People need to understand that businesses have to advertise. Everyone's so worried about individual rights that they are forgetting about society as a whole, forgetting about the whole system... They are a part of that system, and they have to partake in it. They should not be able to opt out for free, because they are opting out of a system that makes money.*[137]

When asked "Do you agree or disagree with the statement: Privacy legislation will just create more red tape for businesses, and that's bad for the economy", 14 percent of British Columbians said they strongly agree, and 41 percent of British Columbians said they strongly disagree.[136]

Most British Columbians do believe that the interests of both consumers and businesses must be considered, but ultimately, they believe that consumers' privacy must be the primary objective of any proposed legislation. As one individual explained,

> *[w]hatever* [privacy protection] *solution B.C. proposes..., it is important to bear in mind that privacy legislation is intended to protect individuals from abuses by those who provide goods and services. The European Directive and other data protection legislation distinguish between data subjects and data controllers. The former are given the rights; the latter the responsibilities. Governments, businesses and professionals are data controllers. It is very important to keep this distinction in mind.*[139]

SELF-REGULATION

Some witnesses to the Committee favour a self-regulatory approach, rather than provincial privacy legislation. For example, one organization wrote that, " a self-regulatory approach is preferable to governmental regulation, since the former provides more flexibility for both industry and regulators and requires fewer public resources to implement."[140] As mentioned, a number of larger businesses and industry associations are also experienced in developing and using their own privacy codes.

When asked, "Do you agree of disagree with the statement: It's more important to protect consumers than to make things easier for business", 77 percent of those who are concerned about information privacy said they strongly agree, and 60 percent of those who said they are not concerned about the issue also agreed with that statement.[138]

> *The Committee heard, however, that for the most part, British Columbians are not convinced that private sector businesses and organizations will adequately manage the privacy of their personal information in the absence of legislation: Overall, legislation was seen as the only viable way to protect information privacy. Although a few participants noted that "it would be nice" if private sector organizations could self-regulate their handling of personal information, participants felt it is simply not realistic to expect all companies to regulate themselves. As long as compliance with basic principles is voluntary, some companies will choose not to follow them.*[141]

Those views are supported by the levels of trust British Columbians indicated for private sector enterprises. Ipsos-Reid asked respondents to rate how much they trust different kinds of private sector organizations to "be careful with information they might have about individuals," and reported the following:

> *approximately one-third say they have a great deal of trust that banks (36%) and credit unions (34%) will be careful with information they may have about them....*

> *Roughly one-in-five say they have a great deal of trust in charitable organizations (22%). Only one-in-seven (14%) say they have a great deal of trust in large retail establishments; one-in-eight (12%) say they trust independent small retailers.*
>
> *While those numbers are low, only half as many express the same level of trust in on-line retailers (7%). Internet services in general also suffer from a significant lack of public trust (just 7% say they trust them a great deal).*[142]

One individual claimed that voluntary guidelines do not provide adequate protection for personal information.[143] Another is even more pessimistic about the ability of businesses to regulate themselves. Commenting on the idea that businesses will adopt privacy protection measures voluntarily because it makes good business sense, this witness said "I would... say that it is in the self-interest of business to *appear* to respect the *genuine* privacy concerns of its customers." [144]

Finally, a number of observers have argued that self-regulation is not an option, given that in January 2004, the *Personal Information Protection and Electronic Documents Act* will cover the provincially-regulated private sectors of provinces that have not passed "substantially similar" provincial legislation.

HARMONIZATION

Recommendation 2:

The Committee recommends that proposed legislation harmonize with other Canadian and international jurisdictions, particularly the federal *Personal Information Protection and Electronic Documents Act*, by establishing a legal framework based on the internationally-recognized fair information principles such as those expressed by the Canadian Standards Association Model Code for the Protection of Personal Information: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

Section 30(2) of the *Personal Information Protection and Electronic Documents Act* stipulates that three years after coming into force, the Act will apply to any organization in the provincial private sectors that collects, uses or discloses personal information. While most private sector activities, except for a range of matters in transportation, telecommunications and banking, are areas of provincial jurisdiction under the division of powers in the *Constitution Act 1967*, the federal government is apparently justifying this provision in the Act as part of its constitutional power to regulate trade and commerce. Another potential justification is the federal government's power to enact laws for the "Peace, Order, and Good Government of Canada", should it be determined that the protection of informational privacy in private sector transaction is a matter of not just provincial, but of national concern.[145] Observers are uncertain as to whether section 30(2) of the Act would withstand a court challenge on the constitutionality of federal regulation of this matter in what are normally areas of provincial authority.

Two witnesses to the Committee discussed the constitutionality of the federal Act's section 30(2). These organizations suggested that the British Columbia government should assess the constitutionality of the Act's provisions that purport to give it jurisdiction over the provincial private sector:

> *"Bill C-6 sets up the federal cabinet as the arbiter to determine if any resulting provincial legislation passes muster and can be considered substantially similar. In other words, if BC chooses to pass privacy legislation which for some reason the federal government considers inadequate, Bill C-6 would still purport to override it. It is hoped that the province will assert its provincial jurisdiction in the face of this dubious federal approach."*[146]

A few others submitted that British Columbia should allow the federal *Personal Information Protection and Electronic Documents Act* to apply to the province. One organization, for example, wrote that:

> *"...the British Columbia government should examine the costs and benefits of adopting separate provincial legislation and consider the possibility of not legislating in this area.... The least costly and simplest outcome for British Columbia businesses and consumers may well be to allow the federal regulatory regime to prevail without additional provincial rules."*[147]

Finally, some told the Committee that the federal law should be considered simply a baseline standard for privacy protection, and that B.C. should not settle for the minimum standard of privacy protection required by the federal legislation.

However, the majority of observers minimize the significance of the federal law's jurisdictional uncertainty, claiming that regardless of the constitutionality of section 30(2), provincial governments, private sector organizations and consumers would see it in their best interests to conform to the fair information principles articulated by the *Personal Information Protection and Electronic Documents Act*.

A large majority of witnesses to the Committee expressed the view that due to the interconnected and dynamic nature of personal data processing and communications, governments must ensure that national and sub-national private sector privacy legislation is consistent, or harmonized, in order to ensure that private sector organizations in all jurisdictions are subject to the same level of regulation, and to guarantee that all consumers can expect the same level of privacy protection. Harmonization is also seen as necessary to simplify the compliance requirements for private sector organizations that operate in more than one jurisdiction. Harmonization is particularly important for provincially-regulated business sectors, as the Insurance Bureau of Canada explained:

> *Although many P&C [property and casualty] insurers are incorporated federally, the authority to regulate insurance operations, including market conduct, rests with the provincial and territorial governments and with their insurance regulators.... Second, the majority of P&C insurers operate in more than one province....*[148]

CSA MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION

The majority of businesses and organizations recommended that any provincial legislation for the protection of information privacy in the private sector be based on the fair information principles of the CSA Model Code. They believe the CSA Model Code provides a good model for harmonized legislation because,

- it contains the ten universally accepted fair information principles that are necessary for personal privacy protection;
- it has achieved a good balance between the interests of consumers and the interests of private sector businesses and organizations; and

- it would help to ensure that any provincial private sector legislation takes the form of sound principles, rather than detailed provisions, which organizations suggested would give legislation needed flexibility in application to various sectors.

Individual British Columbians also expressed their support for the principles underlying the CSA Model Code. For example,

> *In terms of obtaining consumer permission, more than eight British Columbians in ten want the legislation to require that permission be obtained to collect (85%) and share (86%) information about them. Roughly seven-in-ten (68%) would also like the legislation to require permission for the internal use of individuals' information (such as for direct marketing, internal research functions, etc.).*
>
> *In addition to obtaining explicit permission, BC consumers would also like the legislation to require that consumers be informed. Three-quarters (75%) feel it is very important that legislation require that consumers be told how information about them is used and just over eight-in-ten (84%) believe consumers should also have access to their own files so that they can learn what organizations know about them, and take action to correct any errors in that information.*[149]

According to the Information, Science and Technology Agency (ISTA), however, most experts agree that the inclusion of the CSA Model Code in the federal *Personal Information Protection and Electronic Documents Act* has created interpretative confusion. ISTA therefore suggests that while it is essential that the principles expressed in the CSA Model Code be included in provincial privacy legislation, the actual Code itself should not.[150]

SECTORAL CODES OF PRACTICE

Recommendation 3:

The Committee recommends that private sector businesses and organizations be encouraged to develop and adopt privacy codes to assist them in implementing and complying with the fair information principles, and in educating their consumers, clients and employees.

The Committee heard from a several individuals and organizations that privacy legislation for the private sector in British Columbia should allow for the use of industry-specific codes of practice. Sectoral codes, working along with privacy legislation, can help to uphold the fair information principles by

- allowing for flexibility in applying the principles,
- giving various business sectors an opportunity to participate in the development of practical rules,
- providing the details as to how legal obligations will be met in practice, and
- educating organizations and individuals about how legislation will work in day-to-day business transactions.

ISTA stressed that "privacy codes are an effective and complementary companion to legislation. Many businesses have developed codes and have used them with great benefits for raising awareness of privacy in their organizations and for providing an implementation framework."[151]

One organization recommended to the Committee that sectoral codes not have legislative force, but be authorized to assist in the interpretation of legislation for their respective sectors, as in the

Netherlands' privacy protection model. In that model, sanctioned sectoral codes must be approved by an empowered authority.[152]

THE RIGHT TO INFORMATION PRIVACY

Some witnesses recommended that British Columbia "develop legislation from a human rights perspective and establish the fundamental right to privacy as the legal foundation of future legislation."[154] It was also suggested that as technology advances and the potential for privacy abuses increase, information privacy will be best achieved through a technologically neutral, human rights-based privacy law:

> *"Technology innovation and diffusion occur at such a high rate that it is very difficult to anticipate their impact, either short-term or long-term. Thus, the law must inevitably confront situations not anticipated when relevant sections were enacted. Catching up and stretching interpretations has become a way of life. Uncertainty is prevalent. For privacy protection to be effective, privacy must be enunciated as a fundamental right applicable to all identifiable violations."*[155]

British Columbians who are concerned about information privacy express two main rationale. The first is the somewhat vague notion that we simply have a right to privacy (29%). The second is being unable to control how our personal information is used or to whom it is given (26%).[153]

One organization explained that the federal *Personal Information Protection and Electronic Documents Act* is considered adequate for most private sector activities because, having incorporated the CSA Model Code, it includes the requirement to obtain consent for the collection, use and disclosure of personal information. However, this organization argued that rights-based legislation is essential for the protection of personal health information.[156]

JUSTIFICATION OF PURPOSES

The Committee heard from one organization that in order to protect the most fundamental principle of the right to privacy - an individual's ability to control his or her personal information - the "justification principle" must be recognized. Respect for this principle would reinforce the principle of consent by providing individuals with a means of challenging what they perceive to be instances of "forced" consent.

> *"This principle would limit organizations to collecting personal information only when there is a good and legitimate reason to do so. This principle would not only require the organization wanting to gather personal information to state why it needs the information (CSA Model Code principle 2 – purpose), but, if challenged, it would be obliged to justify its request for the information."*[157]

It was noted that section 4 of the Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* includes a justification provision:

> *[A]ny person carrying on an enterprise who may, for a serious and legitimate reason, establish a file on another person must, when establishing the file, enter its object.*

The EU Directive, in Article 6, also contains a justification requirement -

> *Article 6*
> *1. Member States shall provide that personal data must be:*

Netherlands' privacy protection model. In that model, sanctioned sectoral codes must be approved by an empowered authority.[152]

THE RIGHT TO INFORMATION PRIVACY

Some witnesses recommended that British Columbia "develop legislation from a human rights perspective and establish the fundamental right to privacy as the legal foundation of future legislation."[154] It was also suggested that as technology advances and the potential for privacy abuses increase, information privacy will be best achieved through a technologically neutral, human rights-based privacy law:

> *"Technology innovation and diffusion occur at such a high rate that it is very difficult to anticipate their impact, either short-term or long-term. Thus, the law must inevitably confront situations not anticipated when relevant sections were enacted. Catching up and stretching interpretations has become a way of life. Uncertainty is prevalent. For privacy protection to be effective, privacy must be enunciated as a fundamental right applicable to all identifiable violations."*[155]

British Columbians who are concerned about information privacy express two main rationale. The first is the somewhat vague notion that we simply have a right to privacy (29%). The second is being unable to control how our personal information is used or to whom it is given (26%).[153]

One organization explained that the federal *Personal Information Protection and Electronic Documents Act* is considered adequate for most private sector activities because, having incorporated the CSA Model Code, it includes the requirement to obtain consent for the collection, use and disclosure of personal information. However, this organization argued that rights-based legislation is essential for the protection of personal health information.[156]

JUSTIFICATION OF PURPOSES

The Committee heard from one organization that in order to protect the most fundamental principle of the right to privacy - an individual's ability to control his or her personal information - the "justification principle" must be recognized. Respect for this principle would reinforce the principle of consent by providing individuals with a means of challenging what they perceive to be instances of "forced" consent.

> *"This principle would limit organizations to collecting personal information only when there is a good and legitimate reason to do so. This principle would not only require the organization wanting to gather personal information to state why it needs the information (CSA Model Code principle 2 – purpose), but, if challenged, it would be obliged to justify its request for the information."*

It was noted that section 4 of the Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* includes a justification provision:

> *[A]ny person carrying on an enterprise who may, for a serious and legitimate reason, establish a file on another person must, when establishing the file, enter its object.*

The EU Directive, in Article 6, also contains a justification requirement -

> *Article 6*
> *1. Member States shall provide that personal data must be:*

> *(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*

- as does the *Personal Information Protection and Electronic Documents Act* in section 5(3) :

> *[A]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.*

In contrast, another organization put forward that even the identification of purposes principle gives regulators wide powers to review and circumscribe the purposes for which private sector organizations collect personal information. And, as mentioned, private sector businesses and organizations feel strongly that privacy regulation in the provincial private sector must not impede legitimate business activity, including effective marketing and the management of operational risks. For that reason, this organization submitted that any legislation developed for the BC private sector must recognize that,

> *" regulators and private sector organizations will be divided about the legitimate purposes for collecting personal information.... Deciding which interest should prevail over the other will be a delicate task. Like the decision to implement the legislation itself, this task must be premised upon an understanding of our practices and values, which render the legislation a necessary and productive step in our regulatory evolution.... Regulators and politicians alike require a well-developed understanding of these norms and values in order to exercise their judgement and, in turn, explain to the public how it is and why it is that they have done so.*[158]

INTRUSIVE PROCESSES

One organization noted that the BC's public sector privacy legislation pertains only to personal information existing in a record. Therefore, the legislation does not extend the Information and Privacy Commissioner's authority to intrusive information-gathering processes unless the information gathered through such means results in the creation of a record. Some examples of intrusive processes are the collection of bodily fluids or tissue samples, or searches of designated personal areas, such as employee or student lockers.

This organization recommends that private sector legislation cover the processes of gathering personal information, whether or not the information is ultimately converted into a record.[159]

SCOPE OF APPLICATION

Recommendation 4:

The Committee recommends that proposed legislation to protect the information privacy of British Columbians apply to all of the provincially-regulated private sector – all businesses and organizations not falling under the jurisdiction of the BC *Freedom of Information and Protection of Privacy Act* – while recognizing the need for a fair and workable balance between information privacy and the use of personal information for legitimate private sector purposes, as noted in recommendation 1.

Recommendation 5:

The Committee recommends that proposed legislation apply uniformly and consistently to all activities undertaken in the private sector – not limited to "commercial activity" – subject to the exceptions discussed in recommendation 6.

Most witnesses urged the Committee to recommend that any chosen provincial privacy protection regime for the private sector be comprehensive, applying as broadly and consistently as possible to all types of personal information and all types of organizations. One organization argued that privacy legislation for the private sector should provide the same rules whether customer information is collected by an agent or salesperson, or through a company's call centre.[160] Another recommended that regulation be consistent for all data users in the financial services sector, so that no competitive advantage is inadvertently conferred on any one segment of the industry.[161] Ipsos-Reid's research also found that,

> *It would appear that British Columbians would like any legislation to be comprehensive, at least in terms of the kinds of specific information which are included. The extent to which it is important that a specific form of information be addressed clearly reflects the levels of sensitivity assigned to each.*
>
> *A sizeable majority of British Columbians believe that it is very important that legislation address financial (89%) and patient (87%) information. On the other hand, consumer information, which is viewed as significantly less sensitive, is noted as very important by just half (50%) of the population.*
>
> *The majority of British Columbians also seen employee (70%) and internet usage (60%) information as very important to be specifically addressed in any legislation.*[162]

ISTA and other observers note that in the event of the application of the federal *Personal Information Protection and Electronic Documents Act* to a province, the Act would exclude coverage to the employees of the provincial private sector. It has been suggested that the Act excludes coverage of provincial private sector employees because the federal government clearly lacks the constitutional authority to legislate in the area of provincial labour relations.[163] Therefore, in section 4(1) of Part 1 the Act states that:

> *"This Part applies to every organization in respect of personal information that*
>
> *(a) the organization collects, uses or discloses in the course of commercial activities, or*
>
> *(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."*

There is also some uncertainty, by virtue of section 4(1), as to whether the *Personal Information Protection and Electronic Documents Act* will be interpreted as applying to non-commercial activities, such as the activities of charitable and non-profit organizations, professionals and professional firms, or publicly-funded health professionals.[164]

A number of individuals and organizations would like legislators to pass privacy legislation that requires and enforces uniform privacy policies for workplaces. As well, 70 percent of British Columbians believe it is very important that employee information is specifically addressed in any private sector privacy legislation.[165]

In order, then, to guarantee consistent and universal application in the provincial private sector, ISTA recommended that any proposed legislation should *not* restrict its application to only the commercial activities of the private sector. ISTA noted that Quebec's *Act respecting the protection of personal information in the private sector* "applies to all non-public organizations, including non-profit organizations," and that the federal government has accepted that act as "substantially similar."[166]

HEALTH INFORMATION

As mentioned, 87 percent of British Columbians believe that it is very important that legislation address patient information.[167] Overall, witnesses also supported the idea that personal health information collected, used and disclosed in British Columbia's private sector should be protected by privacy legislation, whether it is a privacy law of general application to the private sector or legislation specific to health information. It is also important to them that health professionals and organizations in the private and public sectors be subject to the same privacy standards. As one witness said, "standards obviously need to be consistent between the use of health information in the public bodies regulated under the FIPPA, and in the range of private and semi-private organizations that currently need access to this information for some purposes."[168]

Some supported the health information privacy framework of the Canadian Medical Association's Health Information Privacy Code, which is founded on the principle of informed and voluntary patient consent to the collection, use and disclosure of personal health information in both the public and private sectors. Other frameworks are also being developed. For example, one witness told the Committee about the work of the International Medical Informatics Association in developing and promoting a health information privacy and security policy that can be adopted uniformly around the world. In terms of the cost of building strict security controls into an expansive health information system, this individual commented, "our efforts to decrease health care costs may very well be stifled if people decide to withhold information, falsify information, out of fear -- if we have to deal with incomplete records and so on. So there's a complementary cost, which looms already on this side of the horizon."[169]

Some indicated a preference for separate health information privacy legislation because they feel that the broad privacy principles outlined in general private sector legislation are not appropriate for health information, which is more sensitive than other kinds of personal information.[170] Separate health information legislation would also simplify the privacy rules surrounding the collection, use and disclosure of personal health information in interactions between public and private health agencies. One organization recommended that legislation specifically for the health sector should recognize that health information is necessary for secondary purposes that support the provision of health care and health system management.[171]

Most individuals and organizations told the Committee that they oppose the idea of separate health information privacy legislation. They suggested that health information legislation appears designed to sanction existing uses of personal health information among those agencies that are defined as 'custodians', rather than protect privacy. For example, one witness took issue with the Alberta *Health Information Act*[172] because it applies its privacy provisions not only to patients, but also to health care providers, which he believes contradicts the ostensible "privacy protection" purpose of the legislation.[173] It was also noted that provinces that have or are developing special health information legislation, like Alberta, Saskatchewan, Manitoba and Ontario, have been criticized by groups like the Canadian Medical Association for setting the privacy protection standard lower than with general privacy protection legislation.[174] British Columbia's Information and Privacy Commissioner summarized this perspective on health information legislation by saying, "Some would argue that it's kind of perverse that you have separate legislation to deal with that very sensitive information that actually sets broader parameters for its use and disclosure without informed consent by the specific individual about whom the information has been collected." [175]

Some witnesses recommended that further study be undertaken with respect to the need for separate legislation for health information, since there are persuasive arguments both for and against this option.[176]

Health information in Research

Some organizations are especially interested that any proposed private sector privacy legislation for British Columbia maintain the availability of health information for health research. As one organization explained,

> *since research is so vital to the health system, we recommend that the British Columbia government ensure that any general privacy legislation governing the private sector or any specific privacy legislation relating solely to health information, would not apply to: 'the collection, use or disclosure of personal information for research purposes, including scientific or statistical research, where the information is reasonably necessary for the purposes.'*[177]

In order to protect the privacy of personal health information while allowing access to it for medical or health system research, the definition of "personal health information" must be clearly established. The definition of personal health information has significant implications for what types of information can be collected, used and disclosed without the data subject's consent. For example, one organization asked that "information relating to an individual in the conduct of a business, trade, occupation or profession" be exempt from the definition of "personal health information" so that the health sector can continue to benefit from studies of physician prescribing patterns.[178] That organization noted that Ontario's Information and Privacy Commissioner agreed with the exclusion in her submission to the Ontario Ministry of Health and Long-Term Care on its health sector privacy consultations:

> *we believe the definition of personal health information should be drafted to ensure that information about the employment and business responsibilities, activities and transactions on individual health service providers is not included. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information.*[179]

Another point to clarify in the definition of personal health information is the difference between identifiable and non-identifiable patient information. Identifiable, or "personal" health information is health information that can be identified with an individual person, using name, address, a personal identification number, or any other information that would result in the identification of the data subject. Non-identifiable, or anonymized health information is health information that cannot be used to identify the data subject; identifiers, like name, address or identification number have been removed, or were never collected by the data user, and "there is no possibility of data linking or matching" to re-identify the data.[180] Some kinds of heath research, especially longitudinal research, do require identifiable health information, but some kinds of research need only de-identified and/or aggregated health data.

There is some question as to whether or not the definitions of identifiable and non-identifiable information are adequate given the capabilities current information technologies. As a number of individuals and organizations speaking to the Committee noted, it is generally agreed that "it is impossible to truly anonymize data."[181] For example, if research is being conducted on the de-identified information of a small sample of individuals, an individual could be identified personally by a characteristic unique to him or her within the sample group. De-identified and aggregate data can also be linked with additional personal information to re-identify the original data. Aggregate data is also problematic from a privacy perspective if it "targets a group of individuals who may be distinguished - and possibly discriminated against - on the basis of race, age, sexual orientation, area of residence or other identifying characteristics."[182] It has been suggested that although the terminology normally defines personal information as either identifiable or non-identifiable, due to advances in data linking and data matching, it might be more appropriate to characterize patient information as having "a spectrum of identifiability, ranging from identifiable information, through coded or linkage information, to information [that] is truly anonymous."[183]

Some witnesses suggested to the Committee that the definition of "personal health information" should be drafted so as to exclude de-identified patient information from the privacy rules established in proposed legislation, and to provide criteria for determining when information is identifiable or not. One organization noted that excluding de-identified information would be "consistent with the requirement found in the definition of "personal information" in most access and privacy regimes; i.e. that such information be "about an identifiable individual" prior to attracting the privacy protections of the legislation."[184] It was also suggested that a good way to ensure that anonymized health information is not re-identified is to include a provision in legislation to prohibit data users from re-identifying or data-matching anonymized data.[185]

On the matter of consent requirements for the collection, use and disclosure of personal health information, notable differences emerged. Some organizations told the Committee that new privacy legislation must avoid imposing burdensome consent requirements on health care administrators and providers that would frustrate their ability or willingness to provide identifiable health information to researchers. The assumption is that medical and health research is of such significant social value that the benefits of allowing personal health information to be used without consent outweigh the value of an individual's right to privacy. These witnesses recommended, however, that a proposed privacy law establish security mechanisms for the use of identifiable health information. Security measures might include criteria for determining when personal health information can be used without patient consent, or provisions requiring that personal identifiers be encrypted, that research projects be authorized by ethics boards, and that professional accountability mechanisms be embedded in health and research systems.[186]

Conversely, a number of individuals and organizations said that patient consent for the collection, use and disclosure of personal health information must be the rule. For example, some of these witnesses agreed that the Canadian Medical Association's Health Information Privacy Code provides a good model for the consent of personal health information. Principle 3 of the Canadian Medical Association's Health Information Privacy Code advises that failure to obtain consent for the collection, use, access or disclosure of health information violates a patient's right of privacy, the duty of confidentiality, and the trust and integrity of the patient-practitioner relationship.[187]

These witnesses did acknowledge that in the provision of health services, consent is not always possible. Said one, the locus of control is *"informed consent without limits, in principle, but necessarily with some constraints in practice."*[188] Another suggested that the use of implied consent in medical contexts should be limited and based on an assessment that the patient is fully informed and has implied his or her agreement.

Other witnesses' recommendations for a provincial approach to protecting health information privacy were:

- a requirement for organizations to notify individuals regarding uses of their personal information, including ongoing secondary uses
- security standards for health information systems: linked databases should be based on anonymized records, or some form of privacy enhancing technology should be used to separate patient identity from database records.
- privacy promotion initiatives, including public awareness campaigns, training for staff to achieve specific privacy-enhancing behaviours, and education for decision-makers that will enable them to develop appropriate privacy policies and manage their implementation

ELECTRONIC TRANSACTIONS

Advancement of the "e-commerce" agenda is often cited as a primary reason for passing information privacy legislation for the private sector, and there are indeed some valid concerns about raising levels of consumer confidence in electronic business transactions. For example, Internet retailers and Internet services in general are trusted by fewer British Columbians than any other private sector area measured. Only 7 percent of British Columbians said they trust Internet retailers and Internet services a great deal.[189] As the Retail Council of Canada told the Committee, "the development of e-commerce in Canada to its full potential depends on the development of effective and transparent consumer protection."[190]

One option is to make informed consent a necessary component of privacy protection on the Internet. While most web sites require Internet users to explicitly opt-out if they don't want web sites to gather browsing information, one witness said that web sites should instead require an explicit opt-in. An opt-in provision would give a stronger measure of consent.[191]

Large amounts of personal information can be collected, used and disclosed in non-electronic transactions, and regardless of how information is collected, it can later be processed and transmitted in ways that compromise information privacy. One individual therefore advised the Committee that legislators should not focus on promoting trust in e-commerce at the expense of protecting the privacy of conventional forms of personal information: *"An unfortunate and unintended consequence of Industry Canada's desire to link privacy protection to its larger 'e-commerce agenda' has been to create an impression that C-6 is simply designed to regulate the Internet. BC should try to avoid creating that impression."*[192]

EXCEPTIONS

Recommendation 6:

The Committee recommends that government consider and consult with relevant parties on specific and limited exceptions to proposed legislation, including:

a) "publicly available" information, in order to balance the need for this particular class of personal information to be used for marketing and other purposes, but to protect individuals from obtaining it for purposes harmful to the data subject's well-being, health or safety.

b) personal information for activities relating to journalism, art and literature; law enforcement; emergencies concerning the life, health, security or best interests of an individual; scholarly study; and archival purposes.

c) personal information when required for collecting a debt; complying with a court order; or participating in legal proceedings.

PUBLICLY AVAILABLE INFORMATION

The *Personal Information Protection and Electronic Documents Act* has, in section 7, designated a class of information called "publicly available" information, which refers to personal information found publicly available sources such as telephone directories, court records, and professional registers. Private sector businesses and organizations use personal information from these sources in various ways, for example, to conduct marketing research, create directories, prepare consumer or credit reports, and to conduct private investigations. The Act does not exclude publicly available information from coverage, but section 26(1)(a.1) does allow for the possibility of creating an exemption through the regulations. Colin McNairn and Alexander Scott write that according to the federal *Personal Information Protection and Electronic Documents Act,*

> *The regulations under the Act could specify, by class or otherwise, some or all of the information available from these and other public sources…so that it could continue to be used by an organization without the knowledge or consent of the individuals to whom the information relates. Use in this manner will often be the only practical way of taking advantage of the information for the purposes of the organization. In the absence of regulations specifying particular public information or a particular class of public information, an organization is not free to collect, use or disclose that information without the knowledge and consent of all of the individuals to whom it relates.*[193]

One organization recommended that publicly available information, such as name, phone number and address, be made available for marketing purposes under any new provincial privacy law. That organization noted that it will make the same recommendation to the federal government as it develops the regulations to the *Personal Information Protection and Electronic Documents Act.*[194]

As mentioned, British Columbians have expressed concern about the lack of privacy protection for publicly available information. The committee heard that advertisers can easily access addresses and phone numbers by browsing databases of publicly available information, that private investigators can obtain personal information for clients whose motives are questionable, and that third-party access to unlisted phone numbers and addresses can put individuals at risk.

ISTA told the Committee that, in order to satisfy British Columbians' requirements for effective information privacy protection, any such legislation would have to carefully specify reasonable, defendable and limited exceptions, since exceptions to coverage will enable the collection, use and disclosure of personal information without the data subject's knowledge or consent. ISTA noted that privacy legislation from other jurisdictions may not be exemplary in this instance, particularly the exception for journalistic, artistic and literary purposes.[195] Other observers have said that the exemption for journalistic, artistic and literary purposes in the federal legislation may be interpreted so broadly as to significantly limit the scope of information privacy under the Act.

ARCHIVAL PURPOSES

Section 1 of the federal *Personal Information Protection and Electronic Documents Act* excepts from the general consent requirement the use and disclosure of personal information for "statistical, scholarly or research purposes." The Act also requires that the Privacy Commissioner be informed before every use and disclosure of personal information without consent. The Committee heard from the Archives Association of British Columbia that while information privacy legislation is needed to protect individuals' "human dignity, rights to self-determination, and non-interference in their personal and private affairs":

> *[w]ith the passage of time, the protection of privacy can, under carefully controlled circumstances, begin to give way to society's need for knowledge and understanding of its past actions, accomplishments, and difficulties. As the risk of harm lessens, the potential of benefit from disclosure can be realized.*[196]

The Association recommended that any privacy legislation for BC's private sector contain an exception for archival work relating to "family history, avocational research, and the work of archivists themselves in arranging and describing records," such as the exception provided in the BC *Freedom of Information and Protection of Privacy Act.*[197]

It was also suggested that this Committee reiterate the recommendation of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* to lower the time threshold in section 36(d) of that Act to 70 years, and adopt the Act's same time thresholds in the parallel section of any private sector legislation adopted.

CREDIT REPORTING

The credit reporting sector was one that a number of witnesses discussed. One view was that throughout Canada, the provincial credit reporting statutes that currently regulate credit reporting agencies contain comprehensive provisions for maintaining the privacy and confidentiality of personal information. With respect to British Columbia, it was recommended that the BC government work to have BC's *Credit Reporting Act* recognized as "substantially similar" to the *Personal Information Protection and Electronic Documents Act*; and that consumers be allowed to seek remedies against inappropriate credit reporting only through the BC Registrar of Credit Reporting, rather than a Privacy Commissioner or other oversight agent.[198]

On the other hand, it was remarked that the *Credit Reporting Act* is dated and should be reviewed for its consistency with the privacy provisions of the federal *Personal Information Protection and Electronic Documents Act.* It was suggested that a better alternative might be to repeal the *Credit Reporting Act* and bring the credit reporting industry under the scope of a provincial privacy protection statute, overseen by the Office of the Information and Privacy Commissioner.[199]

Similarly, when he was the BC Information and Privacy Commissioner, David Flaherty suggested that for the purposes of "good housekeeping that accompanies data-protection legislation,"

> *it is my considered view that our provincial* Credit Reporting Act *should be looked at as to whether it meets the minimum standards of fair information practices as we go into the twenty-first century. I also believe that the ultimate responsibility for overseeing the privacy practices of credit bureaus should be transferred from the registrar of credit reporting in the Ministry of Attorney General to the office of the information and privacy commissioner, as has been the case in Quebec since 1994. In my view, this should accompany the extension of the* [Freedom of Information and Protection of Privacy Act] *to the private sector.*[200]

ACCOUNTABILITY

FEES

Recommendation 7:

The Committee recommends that private sector organizations, interest groups and the public be consulted on the appropriateness of fees for administrative services when responding to requests for access to personal information held by private sector organizations. If fees are deemed appropriate to charge, the proposed legislation should require that an estimate be required in advance of proceeding with a response to a request. Proposed legislation might also indicate that requests should be fulfilled in a timely manner.

As explained in the section on "Individual Access", the fair information principles require that an individual is entitled to know what personal information is being held by a business or organization, what it is used for, and to whom it is or has been disclosed, and is given the right to access that information upon request. It indicates further that organizations must provide that information at no cost or at a reasonable cost. The rationale for this principle is that high fees would deter an individual from accessing his or her own personal information, but that it is reasonable to allow businesses and organizations to recover some of the administrative costs that may result from compliance with this rule.

The *Personal Information Protection and Electronic Documents Act* requires that businesses conform to the individual access principle, and with regard to fees states in section 9 that:

> *[a]n organization may respond to an individual's request at a cost to the individual only if*
>
> *(a) the organization has informed the individual of the approximate cost; and*
>
> *(b) the individual has advised the organization that the request is not being withdrawn.*[201]

British Columbia's information privacy legislation for the public sector, the *Freedom of Information and Protection of Privacy Act*, provides individuals with the right to access personal information about themselves from public bodies that hold their personal information. The legislation prohibits public bodies from charging individuals fees for accessing their own personal information, and the Regulations to the Act set out a schedule of maximum fees that can be charged. ISTA has issued "Guidelines for Determination of Fee Estimates" to assist public bodies in calculating fees.

ISTA suggests that individuals and private sector businesses and organizations may also anticipate that a schedule of fees or limits on charges will be established "in order to ensure reasonableness or consistency."[202]

OVERSIGHT

Recommendation 8:

The Committee recommends that proposed legislation provide for an oversight mechanism.

Oversight mechanisms provide the means to monitor and regulate compliance with privacy legislation and establish procedures for resolving complaints and instances of non-compliance. Oversight mechanisms are fundamental components of effective privacy protection systems, since they provide individuals and organizations with consistent formal procedures and an independent and authoritative agent to assist them in applying the fair information principles. ISTA told the Committee that "[t]he lack of independent oversight is often cited as the primary deficiency in self-regulation regimes and has been a main criticism of the United States' "safe harbor" proposal." ISTA also suggested that "[s]ome form of independent oversight will be required to meet the requirement of substantially similar under the [federal] Act and for meeting the standard of adequacy under the EU Data Protection Directive."[203]

The Committee heard that individuals and organizations support the idea that private sector information privacy law should include provisions to hold businesses and organizations accountable for their collection, use and disclosure of personal information. One organization noted that self-regulatory models do not include any enforcement mechanism, and it would improve public confidence in the private sector as a whole if private sector business had to comply with legislation.[204]

When asked about the roles for a regulatory body that might oversee privacy legislation in the private sector, individuals agreed that it should have an advisory role:

> *Participants felt it would be essential for some regulatory body to provide advice to businesses on how to make sure their policies are in compliance with any new legislation. "Otherwise how would they know what to do?" noted one.*[205]

It was also suggested that the powers conferred on an oversight agent for educating the public and undertaking research are important:

> *Under the same 'ounce of prevention' rationale, Commissioners have, and can, act as consultants to organizations that wish to introduce new products and services that may have implications for the protection of personal information. Privacy impact statements can also be an effective tool for the analysis of these implications, to anticipate future problems and encourage a consideration of privacy and security issues at the outset. Linked to this responsibility is the advice that may be given about the use of privacy enhancing technologies.*[206]

Most also agreed that an oversight agent should have the powers to undertake mediation and dispute resolution. Individuals thought "a regulatory body should have enforcement powers or "teeth" in order for legislation to be worthwhile."[207] Some recommended that an oversight agency have the powers necessary to investigate businesses' and organizations' privacy handling procedures, receive complaints, search premises and seize records, subpoena witnesses, and provide remedies for violations.

Several witnesses recommended that legislation for BC should provide for an oversight and compliance mechanism that is general and anticipatory, rather than reactive and remedial. These witnesses told the Committee that pro-active audits are the best way of anticipating and detecting problematic uses of personal information, which often occur without ever being detected by the data subject. One witness therefore claims that compliance auditing is one of the most effective powers of an oversight agency:

> *Under [the Personal Information Protection and Electronic Documents Act] and the [Freedom of Information and Protection of Privacy Act], the Commissioner is given the power of audit: one of the major conclusions of the comparative studies of data protection legislation (by David Flaherty and by myself) is that pro-active auditing is one of the most important functions that a Commissioner can perform.*

Most British Columbians believe that it is very important that businesses and organizations be held accountable to an independent authority (71%).

The Committee heard that even though individuals and businesses generally support the need for an oversight mechanism, they recommend that enforcement of privacy legislation not be too onerous for private sector businesses and organizations. They want any legislation to be straightforward, easy to understand, and easy to administer. For example, meeting the requirements of privacy legislation should not impose a lot of extra paperwork, which adds expense in terms of labour, supplies and filing space, and it should not allow an oversight agent to conduct random audits, which they feel would be invasive and unreasonable.

Businesses seem to be especially apprehensive about compliance with the fair information principle of openness. Some expressed concern that it could expose them to libel or defamation lawsuits, or simply to customer complaints about the information contained in their files. Others are also worried that compliance with the openness principle might be a labour intensive or expensive procedure. There is also some confusion about what it means to provide the consumer with a "reasonable" level of access to their information:

> *Participants we spoke with do not oppose the idea of consumers having access to their own files. However, "reasonable" may be interpreted differently from one business to the next. Aspects of "reasonableness" which may vary from one situation to another include time frame (how quickly must businesses respond to a request for access?) and the level of detail that must be revealed (do companies have a right to keep private any comments on a customer's file?).*

Sufficient funding for an oversight agent is also considered critical.

EDUCATIONAL INITIATIVES

Many individuals and organizations believe that the success of privacy protection depends to a large degree on public education about personal and corporate rights and obligations under the law. It was suggested that an oversight agency, government, private sector businesses and organizations, and the media all have a role to play in educating the public. For example, Ipsos Reid reported that,

> *[p]articipants expected that government should be able to provide them with a plain language overview of what the law allows and prohibits, and, what it means for consumers. Government web sites and pamphlets were cited as the most likely sources for information. One commented however, that mailing out information unsolicited would likely be a waste – pamphlets should be made available on request or, for example, at the post office. Government was also felt to be a trusted source for this information.*
>
> *Participants feel businesses should be responsible for explaining to their customers, employees or clients any changes to their policies in order to comply with the law. Bill inserts and pay stubs were one example of an appropriate venue for either distributing some of this information or referring people to their web sites.*

subject. One witness therefore claims that compliance auditing is one of the most effective powers of an oversight agency:

> *Under [the Personal Information Protection and Electronic Documents Act] and the [Freedom of Information and Protection of Privacy Act], the Commissioner is given the power of audit; one of the major conclusions of the comparative studies of data protection legislation (by David Flaherty and by myself) is that pro-active auditing is one of the most important functions that a Commissioner can perform.*[208]

Most British Columbians believe that it is very important that businesses and organizations be held accountable to an independent authority (71%).[209]

The Committee heard that even though individuals and businesses generally support the need for an oversight mechanism, they recommend that enforcement of privacy legislation not be too onerous for private sector businesses and organizations. They want any legislation to be straightforward, easy to understand, and easy to administer. For example, meeting the requirements of privacy legislation should not impose a lot of extra paperwork, which adds expense in terms of labour, supplies and filing space, and it should not allow an oversight agent to conduct random audits, which they feel would be invasive and unreasonable.[210]

Businesses seem to be especially apprehensive about compliance with the fair information principle of openness. Some expressed concern that it could expose them to libel or defamation lawsuits, or simply to customer complaints about the information contained in their files. Others are also worried that compliance with the openness principle might be a labour intensive or expensive procedure.[211] There is also some confusion about what it means to provide the consumer with a "reasonable" level of access to their information:

> *Participants we spoke with do not oppose the idea of consumers having access to their own files. However, "reasonable" may be interpreted differently from one business to the next. Aspects of "reasonableness" which may vary from one situation to another include time-frame (how quickly must businesses respond to a request for access?) and the level of detail that must be revealed (do companies have a right to keep private any comments on a customer's file?).*[212]

Sufficient funding for an oversight agent is also considered critical.

EDUCATIONAL INITIATIVES

Many individuals and organizations believe that the success of privacy protection depends to a large degree on public education about personal and corporate rights and obligations under the law. It was suggested that an oversight agency, government, private sector businesses and organizations, and the media all have a role to play in educating the public. For example, Ipsos-Reid reported that,

> *[p]articipants expected that government should be able to provide them with a plain-language overview of what the law allows and prohibits, and, what it means for consumers. Government web sites and pamphlets were cited as the most likely sources for information. One commented however, that mailing out information unsolicited would likely be a waste – pamphlets should be made available on request or, for example, at the post office. Government was also felt to be a trusted source for this information.*
>
> *Participants feel businesses should be responsible for explaining to their customers, employees or clients any changes to their policies in order to comply with the law. Bill inserts and pay stubs were one example of an appropriate venue for either distributing some of this information or referring people to their web sites.*

> *Participants felt the news media should also play a role in spreading the word about any new legislation and its potential impact.*[213]

The Insurance Bureau of Canada also advocated that educational initiatives be undertaken to assist with the adoption of any provincial privacy law for the private sector:

> *Public awareness will help to ensure the effective implementation of and compliance with privacy requirements by the private sector. Public awareness can be achieved by independent research, particularly on emerging issues. We cite the example of the federal Privacy Commissioner, who has been very active in researching and publishing reports on relevant topics, making submissions to Parliament and other bodies, and participating in surveys, conferences and symposia.*
>
> *"Public education is the other key function of an effective oversight body. The oversight body should concentrate on educating companies on the advantages of having processes in place to protect the privacy of personal information and, where appropriate, advising companies on how to develop privacy policies and procedures.... The oversight body should also focus on educating the public on what they can do to ensure the protection of their personal information and about the remedies available if they have questions or concerns about a particular company's privacy practices.*

PART 3 BILL 32 — ELECTRONIC TRANSACTIONS ACT

Statutes and regulations governing business conducted in the private and public sectors often indicate that transactions must be documented and authenticated by providing a signature "in writing." As part of the process of adapting to the information economy and supporting e-commerce while protecting information privacy, many jurisdictions are working towards or have introduced measures to establish the legal validity of electronic transactions - transactions undertaken in whole or in part using electronic communications media. For example, the federal government reports that in undertaking this process, the Department of Justice "reviewed over 600 federal statutes and found that 300 of them made references to obtaining or sending information in a way that appeared limited to paper."[214]

In order to ensure that e-business in Canada can reach its expected growth targets, and maintain consistency with the global e-commerce environment, some international organizations have passed legislation authorizing the use of electronic documents in business transactions. In Canada, the federal government enacted electronic transactions legislation as Part 2 of the *Personal Information Protection and Electronic Documents Act*. In the United States, *the Electronic Signatures in Global and National Commerce Act* has come into effect. Saskatchewan, Manitoba, Ontario and Quebec have all introduced or passed similar legislation.

British Columbia must also establish a legal foundation for electronic transactions. Currently in BC, there is some question as to whether electronic documents have the same legal standing as paper documents. In order to achieve the expected growth of e-commerce and to allow government to take full advantage of the promise of electronic service delivery and consequent reductions in red tape, legislation is needed to accommodate electronic signatures and records in accord with other jurisdictions.

While witnesses speaking to the Committee did not address the *Electronic Transactions Act* directly, some stated that legislation to clarify the legal status of electronic transactions is important to the growth of e-business. For example, one business told the Committee that more and more of its customers are accessing the its services through electronic means. The federal Bill C-82, *An Act to Amend Certain laws Relating to Financial Institutions*, has provided for these new service methods by removing references to "written" disclosure in the existing statutes that govern financial institutions, and the *Personal Information Protection and Electronic Documents Act* allows for the use of electronic documents and digital signatures by federal government departments and agencies. This business therefore recommended that British Columbia pass legislation to recognize consent by methods that are appropriate to the nature of new information technologies, such as consent by telephone or by the selection of options on web pages. Another company told the Committee that it is also immersed in the information economy, and that its range of services will continue to expand as new applications are developed for broad-band and Internet-based communications technologies.

The *Electronic Transactions Act* was introduced into the BC Legislative Assembly for first reading on July 5, 2000 for consideration by members of the Legislative Assembly and the public. Part of the mandate of the Special Committee on Information Privacy in the Private sector is to "examine, inquire into and make recommendations with respect to the impact of electronic documents on privacy and freedom of information for British Columbians."[215] Accordingly, the Committee was briefed by representatives of the Information, Science and Technology Agency on the role and impact of the *Electronic Documents Act* on private sector transactions in British Columbia.

The *Electronic Transactions Act* is based on the Uniform Law Conference of Canada's uniform electronic transactions act, which BC and eight other provinces have endorsed as the basis for a consistent e-business legislation across Canada. The Act creates "functional equivalency" between electronic and non-electronic transactions in both the public and private sectors. This means that in both areas, electronic contracts, signatures and documents will be considered as valid in law as their non-electronic counterparts, and when an individual is asked "to provide information in writing, sign a document, produce a document, or retain information or a document", he or she can provide the information using electronic communication.[216] In order to attain functional equivalency between electronic and non-electronic transactions, the Act also establishes rules for conducting and correcting electronic and automated electronic transactions, for establishing "the origin and destination of the record and the date and time when it was sent or received", and the accessibility of an electronic record for subsequent required uses, retention and storage.[217]

The *Electronic Documents Act* is considered "enabling" legislation; that is, it allows individuals, businesses, and government to conduct business electronically, but it does not require the use of electronic communications. The Act says in section 4, that "nothing in this Act requires a person to provide, receive or retain information or a record in electronic form without the person's consent." Section 4 also provides, however, that "consent by a person to provide, receive or retain information or a record in electronic form may be inferred from the person's conduct." This means that when an individual uses electronic communications to interact with government or a commercial organization, the organization may infer that the individual has consented to that form of communication.[220]

An electronic transaction is "any transaction created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic or optical means or by any other similar means. Purchasing a book online from Amazon.com, buying or selling stocks, booking a flight, or applying for a fishing permit on-line are all examples of electronic transactions."[218]

An electronic signature is "information in electronic form that a person has created or adopted in order to sign a record and that is in, attached to or associated with the record...: a digital depiction of a signature block, a user I.D. linked with a password to operate a computer system, and a public "key", a complex algorithm associated with someone's personal identity."[219]

The *Electronic Transactions Act* - like the federal *Personal Information Protection and Electronic Documents Act* - is technology-neutral in that it does not specify that any one authentication technology or form of electronic signature must be used.[221] Some witnesses commented that despite the importance of security in e-commerce, the pace of technological change is such that they do not recommend government pass legislation on the details of encryption, Public Key Infrastructures, or other security measures.

Internationally governments have recognized that encryption technology must be viewed through several policy lenses in order to see all of its implications. According to Industry Canada, consumers want the freedom to choose security software that is affordable and user-friendly. Businesses want to have access to strong security that will protect their business transactions, their corporate information and their intellectual property. They also want consistency in the global marketplace fostered by voluntary solutions. Law enforcement and national security agencies are concerned that if encryption technologies limit their ability to access electronic data in readable form, they could have a negative effect on policing and national security. Civil libertarians and privacy advocates, however, believe that government control of electronic security mechanisms might satisfy law enforcement and national security agencies, but would dampen the exercise of freedom of speech and privacy rights in electronic communications. Canada and other signatories are also bound by

The *Electronic Transactions Act* is based on the Uniform Law Conference of Canada's uniform electronic transactions act, which BC and eight other provinces have endorsed as the basis for a consistent e-business legislation across Canada. The Act creates "functional equivalency" between electronic and non-electronic transactions in both the public and private sectors. This means that in both areas, electronic contracts, signatures and documents will be considered as valid in law as their non-electronic counterparts, and when an individual is asked "to provide information in writing, sign a document, produce a document, or retain information or a document", he or she can provide the information using electronic communication.[216] In order to attain functional equivalency between electronic and non-electronic transactions, the Act also establishes rules for conducting and correcting electronic and automated electronic transactions, for establishing "the origin and destination of the record and the date and time when it was sent or received", and the accessibility of an electronic record for subsequent required uses, retention and storage.[217]

The *Electronic Documents Act* is considered "enabling" legislation; that is, it allows individuals, businesses, and government to conduct business electronically, but it does not require the use of electronic communications. The Act says in section 4, that "nothing in this Act requires a person to provide, receive or retain information or a record in electronic form without the person's consent." Section 4 also provides, however, that "consent by a person to provide, receive or retain information or a record in electronic form may be inferred from the person's conduct." This means that when an individual uses electronic communications to interact with government or a commercial organization, the organization may infer that the individual has consented to that form of communication.[220]

An electronic transaction is "any transaction created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic or optical means or by any other similar means. Purchasing a book online from Amazon.com, buying or selling stocks, booking a flight, or applying for a fishing permit on-line are all examples of electronic transactions."[218]

An electronic signature is "information in electronic form that a person has created or adopted in order to sign a record and that is in, attached to or associated with the record....: a digital depiction of a signature block, a user I.D. linked with a password to operate a computer system, and a public "key", a complex algorithm associated with someone's personal identity."[219]

The *Electronic Transactions Act* - like the federal *Personal Information Protection and Electronic Documents Act* - is technology-neutral in that it does not specify that any one authentication technology or form of electronic signature must be used.[221] Some witnesses commented that despite the importance of security in e-commerce, the pace of technological change is such that they do not recommend government pass legislation on the details of encryption, Public Key Infrastructures, or other security measures.

Internationally governments have recognized that encryption technology must be viewed through several policy lenses in order to see all of its implications. According to Industry Canada, consumers want the freedom to choose security software that is affordable and user-friendly. Businesses want to have access to strong security that will protect their business transactions, their corporate information and their intellectual property. They also want consistency in the global marketplace fostered by voluntary solutions. Law enforcement and national security agencies are concerned that if encryption technologies limit their ability to access electronic data in readable form, they could have a negative effect on policing and national security. Civil libertarians and privacy advocates, however, believe that government control of electronic security mechanisms might satisfy law enforcement and national security agencies, but would dampen the exercise of freedom of speech and privacy rights in electronic communications. Canada and other signatories are also bound by the Wassenaar Arrangement to control the export of cryptography products that might negatively impact the security interests of international allies.[222]

The federal government has been considering the issue of security in electronic transactions since the publication of its electronic commerce strategy in 1998. The strategy outlined a series of initiatives to be undertaken in order to "establish Canada as a world leader in the adoption and use of electronic commerce." (Electronic Commerce in Canada: Canadian Strategy). In addition to the need for a consistent private sector privacy regime, which has been addressed in the *Personal Information Protection and Electronic Documents Act*, the strategy identified a need for policy development on cryptography, authentication, digital signatures, a regulatory framework for e-commerce infrastructures, consumer protection and taxation. In all of these areas, the federal government has been working with the provinces and private sector interests on a comprehensive regulatory foundation for e-commerce.

Canada announced a federal cryptography policy in October 1998 after months of public consultation. In brief, that policy says that:

- *Canadians are free to develop, import and use whatever cryptography products they wish.*
- *The Government will not implement mandatory key recovery requirements or licensing regimes.*
- *The Government encourages industry to establish responsible practices, such as key recovery techniques for stored data.*
- *The Government will act as a model user of cryptography through the practices of the Government of Canada Public Key Infrastructure (GOC PKI).*
- *The Government encourages and supports industry-led accreditation of private sector certification authorities.*
- *The Government proposes amendments to the Criminal Code and other statutes as necessary to:*
    - *criminalize the wrongful disclosure of keys;*
    - *deter the use of encryption in the commission of a crime;*
    - *deter the use of cryptography to conceal evidence;*
    - *apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances.*
- *Canada will continue to implement cryptography export controls in keeping with the framework of the international Wassenaar Arrangement.*[223]

A summary of the federal government's latest consultation process on authentication, which began in July 2000, was published in February of this year as "Addressing the Trust Agenda: Electronic Authentication." It reports that participants strongly agreed that authentication should be regulated by a set of harmonized, high-level principles or voluntary standards. High-level standards would provide guidance and direction to business, confidence to users, and enough flexibility to enable parties to adapt to changing market conditions and new technologies, and to choose the terms and conditions best suited to the kinds of transactions or communications they undertake. In this approach, the government's role would be one of coordination.[224]

Another significant point of consensus on authentication policy was that

> *"a forum should be established for the purpose of developing the principles and that this work should commence in a timely fashion. In approaching this work, stakeholders emphasize the*

> *importance of harmonizing the principles with relevant provincial initiatives to provide for a degree of efficiency and to prevent barriers to inter-provincial trade. It is also recognized that there is a need to ensure that they are compatible with the directions being taken in the various international for a debating the issues associated with authentication-related services so as to position Canada well globally.*[225]

Committee members would like to acknowledge that British Columbia should continue to consult with other provinces in Canada on a harmonized regulatory framework for e-commerce, including cryptography, authentication and digital signatures.

APPENDIX I – IPSOS REID - DETAILED FINDINGS: QUANTITATIVE STUDY

QUANTITATIVE METHODOLOGY

A total of 600 telephone interviews were conducted with a random sample of adult British Columbians, from January 18 to January 23, 2001. These interviews were approximately 15 minutes in duration.

The questionnaire used for the telephone interviews was designed by a senior Ipsos-Reid researcher in consultation with the Office of the Clerk of Committees.

SAMPLE

The sample was drawn proportionately from all regions of British Columbia, and the final results were adjusted (weighted) to ensure an accurate representation of gender and age groups across the province. At a sample size of 600, the results are considered to be accurate to within ±4.0%, 19 times out of 20. That is, we can say that the results are within 8 percentage points of what they would have been had the entire adult population of British Columbia been polled.

For the purposes of analysis, British Columbia was divided into four regions (the total sample size and margin of error are also indicated):

- Lower Mainland (336 interviews, ±5.4%)
- Island/North Coast (107 interviews, ±9.5%)
- South Interior (104 interviews, ±9.6%)
- North Interior (51 interviews, ±13.7%)

ANALYSIS

The data collected in this study was subjected to cross-tabular analysis, that is, we examined the results for each question by a number of variables, including:

- **Demographic:** age, gender, region, income, education and the presence of children in the home
- **Behavioural:** access to the internet
- **Attitudinal:** concern about information privacy at the outset of the interview and concern as expressed at the end of the interview

This report will present the results in aggregate (provincial totals) and will also discuss any statistically significant differences between sub-populations.

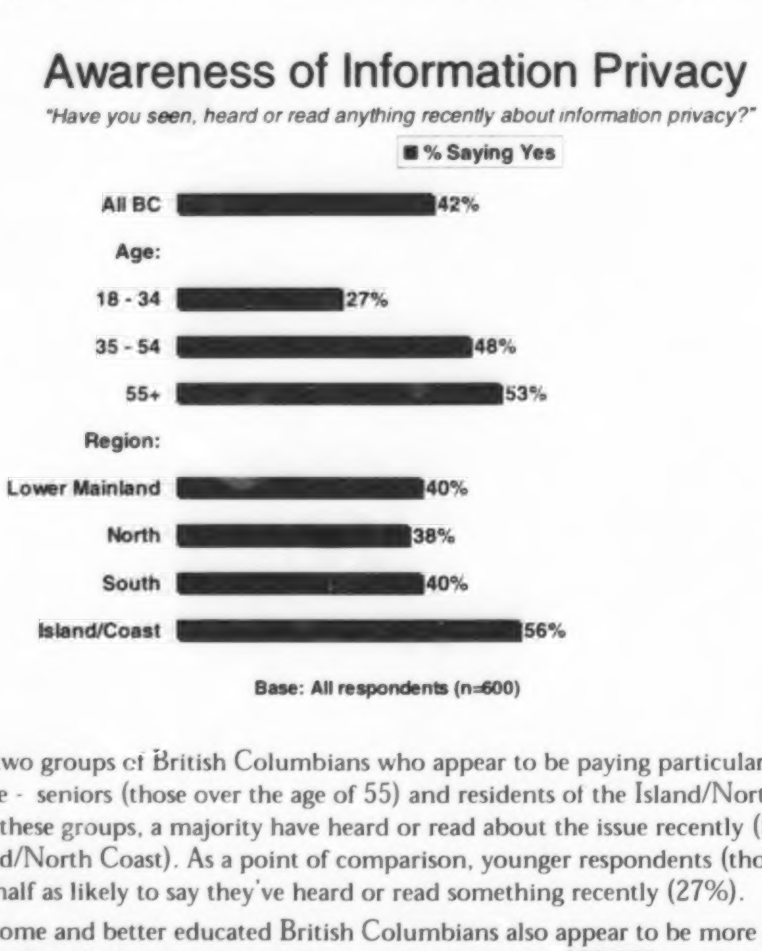
Care should be taken in the extrapolation of results within sub-populations, as the sample size for each is significantly smaller than for the population as a whole, resulting in lower levels of statistical reliability. Nonetheless, these results are indicative of important trends and should not be discounted entirely.

INVOLVEMENT AND CONCERN

British Columbians appear to be paying some attention to the issue of information privacy - nearly half said they had heard or read something about this recently. Clearly, the issue is of some considerable importance as well - an overwhelming majority say they are concerned about this, and for well-considered reasons.

INVOLVEMENT

Just over four British Columbians in ten (42%) say that they have heard or read something recently about information privacy, while nearly six in ten (58%) say they have not. This is not to say, however, that the larger group is unaware of the issue - as we will see, concern about the issue cuts across all groups, and few British Columbians feel unable to offer opinions on the issue.



- There are two groups of British Columbians who appear to be paying particularly close attention to this issue - seniors (those over the age of 55) and residents of the Island/North Coast region. In both of these groups, a majority have heard or read about the issue recently (53%, 55+ and 56%, Island/North Coast). As a point of comparison, younger respondents (those aged 18 to 34) are nearly half as likely to say they've heard or read something recently (27%).
- Higher income and better educated British Columbians also appear to be more involved in this issue - roughly half of university graduates and those earning $60,000 or more (49% each) say they've heard or read something recently. In contrast, roughly one-third of those at the lower end of the economic scale (<$30k, 34%) and who have not attended post secondary studies (High school or less, 34%) say they have heard about the issue recently.

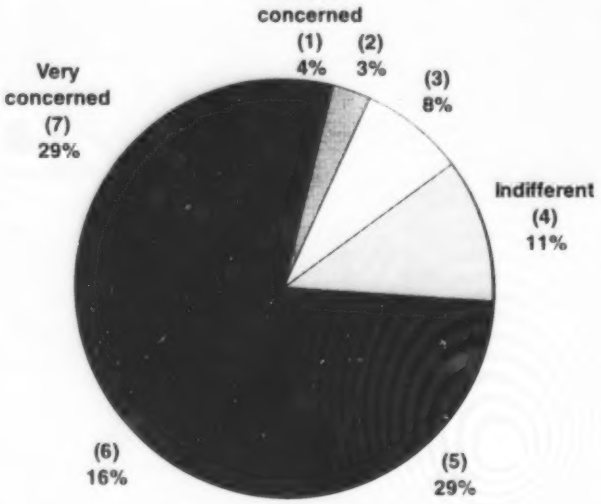
- Interestingly, we see similar levels of involvement among those who are quite concerned about information privacy and those who are less concerned - in other words, it is not only those who are very worried who are paying attention to coverage of the issue.

CONCERN

Most British Columbians (73%) express at least moderate concern about the issue of information privacy. To put this in context, while nearly three in ten (29%) say they are very concerned, fewer than one in twenty (4%) say they are not at all concerned about the issue.

Overall Concern About Information Privacy

*"How concerned are you personally about the issue of information privacy?"**



Base: All respondents (n=600)

*** On a 7-point scale where 1=not at all concerned and 7=very concerned.**

- We noted earlier that Vancouver Island and North Coast residents appear to be more involved in the issue of information privacy than most other British Columbians - they are not, however, particularly worried about the issue. While roughly three-quarters of other British Columbians express at least moderate concern about this issue, fewer than two-thirds (63%) of Island/North Coast residents say the same. Further, only one in five say they are very concerned (20%) compared with more than one-third (36%) of residents of the Northern Interior of the province.
- On the other hand, it seems that older British Columbians are paying closer attention to the issue because they are more concerned. Nearly four in ten (39%) of those aged 55 or older say they are very concerned, this is nearly three times the proportion of the youngest group (16%, 18-34).
- There is a slight gender gap on the issue as well - women are more likely to say they are concerned (77% vs. 69% of men).

RATIONALE FOR CONCERN OR LACK THEREOF

The following table illustrates the reasons that British Columbians offer for their level of concern about information privacy.

Rationale	**Concerned (Base = 440)**	**Indifferent (Base = 67)**	**Unconcerned (Base = 90)**
I have a right to privacy	29%	7%	5%
Lack of control over my information	26%	11%	1%
Selling lists / junkmail	18%	13%	6%
Credit card or other financial information at risk	16%	7%	6%
Internet (general)	12%	11%	10%
Government / "Big brother" having access to too much information	9%	6%	2%
Medical or health information	8%	2%	3%
Fear of misuse of information / concern it will be used against me	4%	10%	--
Fear of exploitation	3%	3%	--
Need more legislation / regulation	3%	--	--
Social Insurance Number	2%	4%	--
Not concerned, have nothing to hide	2%	21%	50%
Sometimes it's necessary to share information	1%	7%	2%
Nothing / no reason	--	--	2%
Other specific reasons	4%	13%	11%
Don't know	1%	2%	9%

Based on a 7-point scale where 1 means "not at all concerned" and 7 means "very concerned." For the sake of analysis, "concerned" includes those who assigned scores of 5, 6 or 7, "indifferent" includes those who assigned a score of 4 and "unconcerned" includes those who assigned scores of 1, 2 or 3.

British Columbians who are concerned about the issue of information privacy, in other words, the majority of British Columbians, have two main rationale for that concern. The first is the somewhat vague notion that we simply have a right to privacy (29%); the second is being unable to control how our personal information is used or to whom it is given (26%).

The majority of those who say they are not particularly worried about information privacy say it is because they simply have nothing to hide (50%, unconcerned, 21%, indifferent).

In addition, concerned British Columbians express a number of worries relating to how information is used. Nearly one in five (18%) are concerned about their information being sold, and receiving junk mail or other unsolicited communication / information as a result; a further one in ten (9%) dislike the idea of "big brother" knowing too much about them and one in twenty (4%) worry that there is the potential for information to be used against them in some way.

The internet, and all of its associated problems and issues, is an important cause for concern among all British Columbians. Interestingly, those who claim to be unconcerned about the issue are as likely as those who say they are very concerned to raise the internet as a rationale for their opinion.

In addition to the ways information might be used or shared, British Columbians also identify specific kinds of information as cause for concern. Those who worry most about the issue of information privacy in general are also the most likely to worry about specific kinds of information. For example, credit card or other financial information is a major worry for this group (16%, vs. 7% of indifferent and 6% of unconcerned). As well, medical and health information is important to roughly one in ten of the most concerned, but of little apparent importance to other British Columbians (8%, concerned vs. 2%, indifferent and 3%, unconcerned).

- Women who are concerned about the issue are more likely than men to cite their right to privacy (34% vs. 24%) while men are more likely to cite concern about lack of control over how their information is used (32% vs. 21%).
- Those with only a high school education are also more likely to say they have a right to privacy (39% vs. 24% of university grads); better educated respondents are more concerned about control (31%, university graduates vs. 19%, high school or less) and issues relating to the internet (16% vs. 8%).
- Interestingly, respondents with no internet access are as likely as those who have access either at home or at work to say that the internet is the main reason they worry about information privacy (13%, none; 13% work; 10%, home).

SENSITIVITY OF SPECIFIC INFORMATION

Before we begin our discussion of the kinds of information which British Columbians feel are most relevant to the issue of information privacy, it is important to discuss the terms that they use to define these various kinds of information. "Personal information," as defined by the respondents to this study, includes information that is applicable to the individual and by which they can be categorized as people. Age, gender, religious affiliation and ethnicity are the main components of this category. We have, for the sake of clarity for the committee, relabelled this information as "Individual Information."

Relevant Information

The following table illustrates the kinds of information which British Columbians think of as relevant to a discussion of information privacy - that is, the kind of information that occurs to them first when asked to think about the issue of information privacy. This question was asked in an unaided manner; respondents were not read a list of choices, but rather offered the responses that occurred to them naturally.

Kind of Information	**% Mentions**
Financial	55%
Medical / health	33%

Individual (age, gender, ethnicity)	27%
Credit card	19%
Identifying (name, address, phone number)	14%
Shopping habits	11%
Social insurance number	8%
Internet usage	7%
Employment records	6%
Credit record	5%
Criminal records	4%
Government records (income tax, birth certificate, citizenship)	4%
Political party affiliation	2%
Charitable donations	1%
Other	6%
Don't know	6%
Multiple response question, total is more than 100%	

Most British Columbians consider financial information as key to a discussion of information privacy; this reinforces the findings of the focus groups, where concerns about credit card information and credit records, as well as access to banking and other financial information were foremost on the minds of participants.

Over half (55%) of BC residents mentioned general financial information as being pertinent to a discussion of information privacy; an additional one in five mentioned credit card information (19%) and one in twenty (5%) mentioned credit records.

- Older respondents are more likely to be thinking about financial matters in general when thinking about information privacy (64%, 55+ vs. 45%, 18-34); younger respondents are more likely to be thinking about their credit card information (25%, 18-34 vs. 14%, 55+).
- Those who are most concerned about the issue of information privacy are also the most likely to mention financial information as being particularly relevant to this discussion (59% vs. 44% of those who say they are not concerned).

Medical and other health-related information is also on the minds of BC residents - one-third (33%) thought of this issue as relevant to a discussion of information privacy. Interestingly, this cuts equally across all demographic sub-groups, with all British Columbians being roughly equally likely to raise the issue.

Individual (27%) and identifying (14%) information were also raised by many British Columbians as being relevant to this discussion.

- Only University Graduates were significantly more likely than the norm to mention individual information (i.e.: gender, age, ethnicity) as being particularly relevant to this discussion (37%, as compared with 27% overall and just 22% of those with high school or less).

Keeping Information Private

A desire to protect financial information appears to be driving many British Columbians' overall concern about the issue of information privacy. An overwhelming majority of British Columbians feel that it is very important that their financial (89%), credit card (88%) and credit record (74%) information be kept private. Not too surprisingly, there is also a significant majority (76%) who believe that medical information must be kept private.

A clear majority also feel it is very important to protect the privacy of identifying information such as name, address and phone number (55%). The majority of British Columbians also feel that internet usage (52%) and employment records (51%) must be kept private.

Interestingly, although people see individual information as being relevant to a discussion of information privacy, only a little more than one-third (37%) feel it is very important to keep information such as age, gender or ethnicity private. The same proportion want information on charitable donations kept private (37%).

At the bottom of the list, in terms of sensitivity, are information about memberships and affiliations (30%) and shopping habits (28%).

Kind of Information	**% Very important to keep private**
Financial	89%
Credit card	88%
Medical or health	76%
Credit record	74%
Identifying (name, address, phone number)	55%
Internet usage	52%
Employment records	51%
Charitable donations	37%
Individual (age, gender, ethnicity)	37%
Membership (political party, other clubs or organizations)	30%
Shopping habits	28%

Based on a 7-point scale where 1 means "not at all important" and 7 means "very important." For the purposes of analysis, "Very important" includes those who assigned scores of 6 or 7.

- We see an important gender gap on the issue of the relative importance of keeping identifying information private. Women are significantly more insistent than men that this information - also known as "directory information," including name, address and phone number - must be kept private. Nearly half of women assign the highest possible level of importance to keeping their identifying information private (47% assigned a score of 7 on the 7 point scale, compared with just 33% of men).
- Just as younger respondents (18-34) are less concerned about the issue of information privacy in general, they are also less inclined to want specific kinds of information to be kept private. Older

respondents (35+) are more protective of their financial information (91% vs. 84%), employment records (59% vs. 42%), identifying information (57% vs. 49%) and, interestingly, internet usage (58% vs. 40%).

- There are only a few regional differences of note. Residents of the Lower Mainland are more protective of their financial (92% vs. 81%, Vancouver Island) and credit card information (91% vs. 83%, South Interior).
- Better educated British Columbians tend to be more concerned about protecting the privacy of most specific kinds of information with one important exception; while half (49%) of university graduates say it is very important that their identifying information be protected, nearly two-thirds (64%) of those with high school or less say the same.
- Those who have internet access only in the home are the most protective of their internet usage information (59% vs. 48% of those with access at work).

TRUST OF BUSINESSES AND ORGANIZATIONS

Although medical and health information is something that the vast majority of British Columbians want kept private, it would appear that most do not feel that their health information is at risk. Of all of the kinds of businesses and organizations examined in this study, those involved in the direct delivery of health services were by far the most trusted.

A majority of British Columbians say they have a great deal of trust in individual health care providers (61%), hospitals (53%), pharmacies (52%) and medical labs (48%). As a point of comparison, insurance companies, which would also have access to health information, are well trusted by only one British Columbian in five (19%).

Financial information was the most pressing concern for British Columbians, in terms of ensuring it is kept private. However, only approximately one-third say they have a great deal of trust that banks (36%) and credit unions (34%) will be careful with information they may have about them.

As we all know, however, our financial information (especially credit card information, a pressing concern for many) is available through a number of different avenues, including charitable organizations and especially through the retail sectors - both "bricks and mortar" and on-line retailers. And it is those organizations which British Columbians trust least to be careful with information about individuals.

Roughly one-in-five say they have a great deal of trust in charitable organizations (22%). Only one-in-seven (14%) say they have a great deal of trust in large retail establishments; one-in-eight (12%) say they trust independent small retailers.

While those numbers are low, only half as many express the same level of trust in on-line retailers (7%). Internet services in general also suffer from a significant lack of public trust (just 7% say they trust them a great deal). Aside from financial information (credit cards in particular), internet services have access to significant amounts of information about us, ranging from our identifying and individual information to our internet usage information, all of which is of some concern to many BC residents.

Business or organization	% Distrust a great deal	% Trust a great deal
Individual health care professionals	9%	61%
Hospitals	9%	53%
Pharmacies	9%	52%
Medical laboratories	11%	48%
Banks	19%	36%
Credit unions	14%	34%
Charitable organizations	21%	22%
Insurance companies	28%	19%
Large retail stores	35%	14%
Independent small retailers	29%	12%
Internet services in general	54%	7%
Internet retailers	59%	7%

Based on a 7-point scale where 1 means "do not trust at all" and 7 means "trust completely." For the purposes of analysis, "distrust a great deal" includes those who assigned scores of 1 or 2 and "trust a great deal" includes those who assigned scores of 6 or 7.

- On the whole, women are more trusting than men of most of the organizations we examined in this study. One interesting exception to this is the case of banks versus credit unions. While women are far more trusting of banks than are men (44% trust a great deal, vs. just 28% of men), men and women are equally trusting of credit unions (35% and 34% respectively).
- Lower income respondents are more trusting of charitable organizations than their higher income counterparts (35%, <$30k vs. 17%, $30-$60k).
- Better educated respondents tend to be less trusting of all of the businesses and organizations included in this study. In most cases, the difference is slight, but there are others which are quite striking; university graduates are half as likely as high school graduates to say they trust small retailers a great deal (5% vs. 13%). Importantly, they are also less likely to trust hospitals (47% vs. 59% of those with post secondary certificates or incomplete degrees).
- Not surprisingly, those who are not concerned about information privacy tend to express higher levels of trust in various businesses and organizations. For example, 78 percent say they trust individual health care providers a great deal, as compared with 66 percent of those who are "indifferent" and 57 percent of those who are concerned. There are some cases, however, when they are not significantly more trusting than other British Columbians. For example, there is no real difference in the level of trust of internet and independent small retailers; and there is also no real difference in the level of trust in medical laboratories or pharmacies.

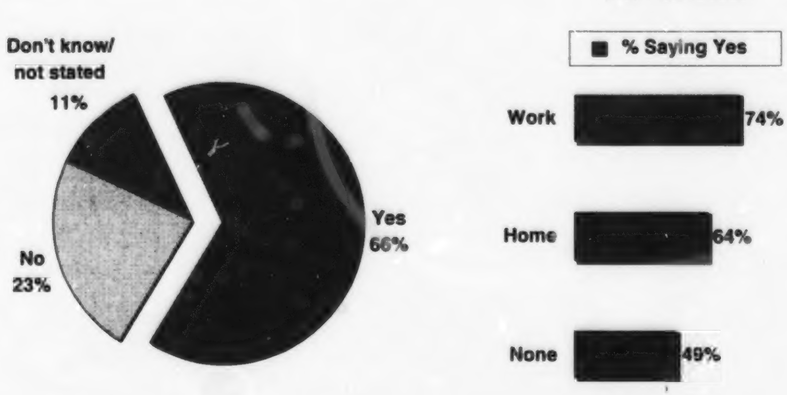
LEGISLATION: AWARENESS AND PERCEIVED NEED

AWARE OF CURRENT STATUS

Most British Columbians believe there is currently some form of legislation or regulation in place to protect individuals' information privacy, and the vast majority also feel that there is a real need for this kind of legislated protection.

Aware of Legislation

"To the best of your knowledge, are there any laws or regulation s here in BC that protect individuals' information privacy?



Base: All respondents (n=600)

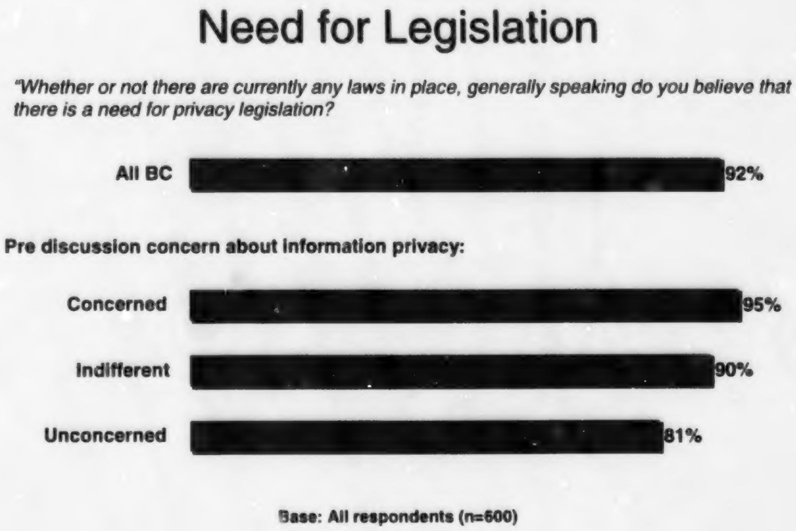
Fully two-thirds (66%) believe there are laws or regulations in place in BC to protect our information privacy; just under one-quarter (23%) say this is not true and one-in-ten (11%) are uncertain.

- Older respondents are less likely to believe that laws currently exist, especially as compared with those in the middle age group. While seven in ten (71%) of those aged 35 to 54 say that there are laws in place in BC, just six-in-ten (59%) of those over 55 say the same.
- Better educated respondents are also more likely to say there is legislation (76% of university graduates vs. just 51% of those with high school or less).
- Those with internet access, either at home (64%) or at work (74%) are more likely than those with no access (49%) to say that legislation exists now in BC.
- Parents are also more inclined to believe that legislation currently exists (72% vs. 62% of those without children under the age of 19).
- There is an interesting comparison to be made in pre and post survey concern. Looking at pre-survey concern, one sees no real difference in the likelihood that respondents believe there is currently legislation in place (roughly two-thirds of all three groups contend that this is the case). However, when we look at those who say in post-survey questioning that they are not concerned about the issue, this group is far more likely than all others to express confidence that privacy legislation currently exists (81%, vs. 64% of those who are concerned in post-survey

questioning). In other words, those who believe there is legislation in place are less concerned about information privacy after taking part in a discussion of the issue. It is possible that their level of concern is diminished after being "reminded" that there is legislation.

NEED FOR LEGISLATION

Certainly, there is no question that British Columbians perceive a real need for legislation to protect information privacy. Just over nine-in-ten (92%) say that this is true, versus just one-in-twenty (6%) who contend that *"businesses and other organizations can be trusted to do the right thing without there being any laws."*



- On the whole, this perception that there is a need for legislation cuts equally across all sub-populations, with one minor, and not unexpected, exception. People who tend to be less concerned about the issue of information privacy (whether in pre or post survey questioning) are slightly more likely to trust businesses to do the right thing without legislation (pre-survey, 16% not concerned vs. 3% concerned; post-survey, 15% not concerned vs. 4% concerned).

ROLE OF INTERNET IN NEED FOR LEGISLATION

Even though a majority (69%) believe that the new information technologies make it impossible to be positive that our information is completely protected, it is for this very reason that an even larger majority (80%) hold that we must have privacy legislation.

Role of Internet	**% Strongly agree**
The internet has made it more important than ever that information privacy be protected	80%
With the internet and other new technology, it's impossible to be completely certain that personal information is kept completely private	69%
Based on a 7-point scale where 1 means "strongly disagree" and 7 means "strongly agree." For the purposes of analysis, "strongly agree" includes those who assigned scores of 6 or 7.	

- Respondents living in the Northern Interior (89%) and those in the middle age category (84%) are the most likely to strongly believe that the internet has made it even more important that we have information privacy legislation.
- Those who have internet access only at home are the most likely to worry that it is now impossible to be certain our information is kept private (76%). In contrast, those with access at work are the least likely to strongly agree that this is true (66%). Interestingly, the presence of children in the home appears to have no impact on opinion on this question (69% each, children and no children).

LEGISLATION: PRIORITIES, FUNCTION AND IMPACT

PRIORITIES FOR KINDS OF INFORMATION

It would appear that British Columbians would like any legislation to be comprehensive, at least in terms of the kinds of specific information which are included. The extent to which it is important that a specific form of information be addressed clearly reflects the levels of sensitivity assigned to each.

A sizeable majority of British Columbians believe that it is very important that legislation address financial (89%) and patient (87%) information. On the other hand, consumer information, which is viewed as significantly less sensitive, is noted as very important by just half (50%) of the population.

The majority of British Columbians also seen employee (70%) and internet usage (60%) information as very important to be specifically addressed in any legislation.

Kind of Information	**% Very important to include in legislation**
Financial	89%
Patient	87%
Employee	70%
Internet usage	60%
Consumer	50%
Based on a 7-point scale where 1 means "not at all important" and 7 means "very important." For the purposes of analysis, "Very important" includes those who assigned scores of 6 or 7.	

- In most cases, the youngest respondents are also the least likely to feel it is very important for a specific kind of information to be included in legislation. For example, just under half (47%) of those aged 18 to 34 feel that it is very important for the legislation to address internet usage information, compared with two-thirds of those aged 35 or older (66%). Similarly, while just over half of those over the age of 35 would like to see consumer information protected (56%), just over one-third of the youngest group feels the same (36%).
- Men and women are generally in agreement on the kinds of information which should be included in legislation, with one exception. Women are far more likely than men to say that it is very important to include employee information (74% vs. 65% respectively).
- Those who have attained high school matriculation or less are more likely to want internet information (67% vs. 55% post sec or university grads) and consumer information (59% vs. 42% university grads) included in legislation.

PRIORITIES FOR THE REQUIREMENTS OF THE LEGISLATION

British Columbians would also like any legislation to be fairly comprehensive in its scope in terms of the requirements that it makes of businesses and organizations. A sizeable majority believe that it is very important that the legislation address all of the various requirements presented in this study, ranging from requiring that internet transactions are protected to obtaining consumer permission to use information in a variety of ways.

In terms of obtaining consumer permission, more than eight British Columbians in ten want the legislation to require that permission be obtained to collect (85%) and share (86%) information about them. Roughly seven-in-ten (68%) would also like the legislation to require permission for the internal use of individuals' information (such as for direct marketing, internal research functions, etc.).

In addition to obtaining explicit permission, BC consumers would also like the legislation to require that consumers be informed. Three-quarters (75%) feel it is very important that legislation require that consumers be told how information about them is used and just over eight-in-ten (84%) believe consumers should also have access to their own files so that they can learn what organizations know about them, and take action to correct any errors in that information.

Given the level of concern about internet information, it is not surprising that there is a very strong appetite for the legislation to require that all internet transactions be protected (87% feel this is very important).

Finally, when it comes to ensuring that these requirements are followed, most British Columbians also believe that it is very important that businesses and organizations be held accountable to an independent authority (71%).

Options for requirements of the legislation	% Very important
Ensure that all internet transactions are protected	87%
Obtain individuals' permission to share information with outside organizations	86%

Obtain individuals' permission to collect information about them	85%
Provide access to individuals to information about themselves and allow them to correct errors	84%
Inform consumers how they use information about them	75%
Be accountable to an independent authority	71%
Obtain individuals' permission to use information internally, such as for sales, marketing or research	68%
Based on a 7-point scale where 1 means "not at all important" and 7 means "very important." For the purposes of analysis, "Very important" includes those who assigned scores of 6 or 7.	

- While clearly supportive of these requirements, younger respondents are slightly less insistent that all they be included. For example, while three-quarters (73%) of those aged 55 or older say it is very important for legislation to require that permission be obtained for the internal use of individual's information, just six-in-ten younger respondents feel the same (61%, 18-34).
- Those in the middle age group are the most insistent about accountability - more than three-quarters (78%, 35-54) say it is very important that businesses and organizations be held accountable to an independent authority, compared with less than two-thirds (62%) of younger respondents.
- University graduates are slightly less insistent that the legislation require that permission be obtained for the internal use of information (63% vs. 73% of those with only a high school education).

PRIORITIES FOR APPLYING THE LEGISLATION

Most British Columbians also want the legislation to be consistent and consistently applied - from province to province and from business to business.

A clear majority strongly believe that the laws should be the same across Canada and that they should be the same for all businesses and organizations, regardless of their size or the nature of their business (86% and 74% respectively).

As well, a clear majority (75%) strongly believe that private sector organizations should be subject to the same information privacy laws as the public sector (government).

Options for applying legislation	**% Strongly agree**
Businesses and organizations across Canada should be subject to the same information privacy laws, not different laws from province to province	86%
Private sector businesses and organizations should be subject to the same information privacy laws as government and government agencies	75%

All types of private sector businesses and organizations should be subject to the same information privacy laws, regardless of their size or the nature of their business	74%
Based on a 7-point scale where 1 means "strongly disagree" and 7 means "strongly agree." For the purposes of analysis, "strongly agree" includes those who assigned scores of 6 or 7.	

- British Columbians across all regions and demographic sub-groups are looking for consistency in information privacy legislation. Only those who are generally more concerned about the issue of information privacy stand out in this matter, in that they are the most likely to strongly agree that all three of these contingencies be applied.

Potential Impact on Business

When it the potential impact of information privacy legislation, British Columbians tend to be quite optimistic. Most agree that businesses will be helped by this kind of legislation, in that consumers will trust them more (52% strongly agree, just 8% strongly disagree). Very few believe that legislation will create red tape that will hurt the economy (just 14% strongly agree while 41% strongly disagree). Further, this optimism may be behind the widely held opinion that it is more important to protect consumers than to make things easier for business (73% strongly agree).

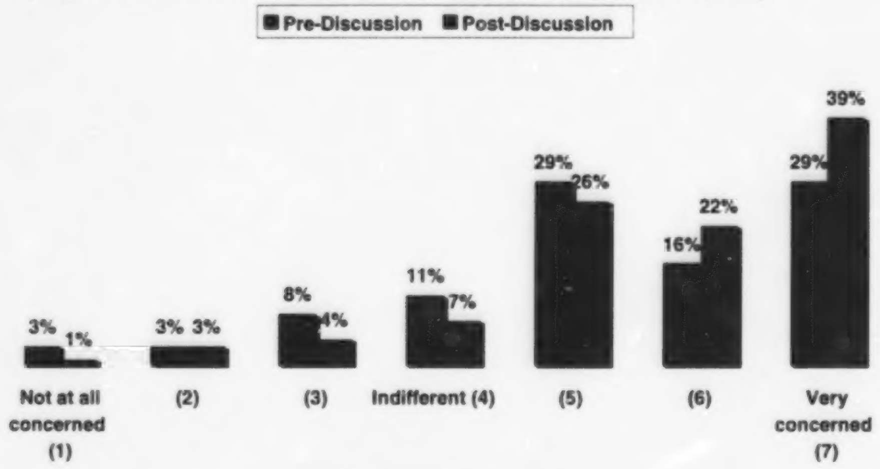
Impact on Business	**% Strongly agree**
It's more important to protect consumers than to make things easier for businesses	73%
Privacy legislation will help businesses in the long run, because consumers will trust them more.	52%
Privacy legislation will just create more red tape for businesses and that's bad for the economy	14%
Based on a 7-point scale where 1 means "strongly disagree" and 7 means "strongly agree." For the purposes of analysis, "strongly agree" includes those who assigned scores of 6 or 7.	

- Older respondents are slightly less optimistic about the potential impact of privacy legislation. Nearly one-quarter of seniors (22%, 55+) strongly agree that legislation will result in red tape that can hurt the economy - this is double the proportion of younger respondents (11%).
- Women are more likely to feel that businesses will actually be helped by this legislation (56% strongly agree that consumers will be more trusting, vs. 46% of men).
- Lower Mainland residents are also more likely to believe that businesses will be helped (55% strongly agree, vs. 44% of Vancouver Island/North Coast residents).
- More than three-quarters (77%) of those who are concerned about information privacy strongly agree that protecting consumers is more important than making things easier for business. In contrast, roughly six-in-ten (59%) of those who say they are not concerned about the issue feel the same.

CONCERN ABOUT INFORMATION PRIVACY – BEFORE AND AFTER

Discussion of the issue of information privacy appears to increase overall concern about the issue. Where 29 percent of British Columbians expressed extreme concern about information privacy at the outset of the interview, fully 39 percent expressed the same level of concern at the completion of the discussion.

More than one-tenth of those who said they were not concerned about the issue at the beginning of the survey had changed their position to one of extreme concern after discussing the issue (12% of those who assigned scores of 1, 2 or 3 on the 7-point scale at the beginning of the interview assigned a score of 7 at the end of the interview).



Comparing Concern – Pre & Post Discussion

"And finally, thinking about everything that we've discussed today about information privacy, please tell me how concerned are you personally about the issue of information privacy.

Base: All respondents (n=600)

- It appears that discussion of the issue of information privacy has a greater impact on younger than on older British Columbians. Where just 63 percent of those aged 18 to 34 expressed concern at the outset of the survey, 82 percent said the same at the end - a jump of 19 percentage points. This is almost double the change among older respondents (11 points from 77% to 88%, 35-54).
- Lower income respondents also appeared to be dramatically affected by this discussion, moving from 69 percent to 86 percent concern.

APPENDIX II – SURVEY

Hello, this is ____________________ calling from Ipsos-Reid, formerly called the Angus Reid Group. We're a professional public opinion research company. Today we're talking to a random sample of British Columbians about some important issues facing our province. Let me assure you that I'm not calling to try to sell you anything, it's just a survey that will take about 15 minutes to complete. I'd like to speak to the person in your household who is 18 years of age or older, and who had their birthday last. Is that you?

Yes **(CONTINUE)**

Don't Know **(ASK AGAIN, IF STILL DK/REF THEN THANK AND TERMINATE)**

No

May I speak to that person? **(READ INTRODUCTION)**

Do you or anyone in your household work for a company that does work in **(READ LIST)**

Media

Marketing research

Advertising

Public Relations

(DO NOT READ: None) **(IF YES TO ANY, THANK AND TERMINATE, IF NONE, CONTINUE)**

(DK/NS) **(THANK & TERMINATE)**

SEX: **(DO NOT ASK - WATCH QUOTAS)**

Male

Female

1. Today we're going to be talking about information privacy. Have you seen, heard or read anything recently about information privacy?
    - Yes
    - No
    - Don't know/refused

READ TO ALL:
As you may know, there has been some discussion lately about information privacy, that is, about how businesses and other organizations use and protect information that they have about individuals, such as consumers, employees, patients, and so on.

2. Generally speaking, and based on what you know, or what you have heard or read, how concerned are you personally about the issue of information privacy? Please use a scale from 1 to 7 where 1 means you are not at all concerned and 7 means you are very concerned.
3. What is the main reason you say that? (PROBE: RECORD VERBATIM RESPONSE)

4. What kinds of information do you think about when you hear people talking about information privacy? (DO NOT READ LIST: ACCEPT UP TO 3 RESPONSES)

- Personal information (age, gender, ethnicity)
- Identifying information (name, address, phone number)
- social insurance number
- credit card information
- credit record
- financial information (income, bank account)
- internet usage
- medical/health information
- employment records
- shopping habits
- political party affiliation
- charitable donations
- other (specify)
- don't know

5. I am going to read you a list of different kinds of information that businesses and other organizations might have about you, and I'd like you to tell me how important it is to you that that information be kept private. Please use a 7 point scale, this time where 1 means it is not at all important and 7 means it is very important. The first one is (READ ITEM - RANDOMIZE). What about (READ NEXT ITEM)?

- Personal information (such as age, gender, ethnicity)
- Identifying information (such as name, address, phone number)
- Credit card information
- Credit record
- Financial information (such as income, bank account, credit card)
- Internet usage
- Medical or health information
- Employment records
- Shopping habits (such as where you shop and what you buy)
- Membership (such as in clubs or organizations)
- Charitable donations

6. There are a wide range of kinds of businesses and organizations that might have information about individuals. I'd like to know how much you trust each of the following organizations to be careful with information they might have about individuals. Please use a 7 point scale where 1 means that you do not trust them at all and 7 means that you trust them completely. The first one is (READ ITEM - RANDOMIZE). What about (READ NEXT ITEM)?

- Banks

- Credit unions
- Charitable organizations, such as the United Way, Cancer Society and so on
- Large retail stores, such as Safeway, Eatons or The Bay
- Independent small retailers
- Internet retailers
- Internet services in general, such as websites, internet service providers and so on
- Individual health care professionals, such as doctors, dentists, massage therapists and so on
- Hospitals
- Medical laboratories
- Pharmacies
- Insurance companies

Now we're just going to change the subject slightly.

7. To the best of your knowledge, are there any laws or regulations here in BC that protect individuals' information privacy?

   - Yes
   - No
   - Don't know

8. Whether or not there are currently any laws in place, generally speaking do you believe... (READ LIST, RANDOMIZE, ACCEPT ONE RESPONSE ONLY)?

   - that there is a need for legislation to cover information privacy
   - that businesses and other organizations can be trusted to do the right thing without there being any laws

   (DO NOT READ: it depends)
   (DO NOT READ: don't know)

READ TO ALL:
As you may or may not be aware, information privacy legislation is being developed in some provinces in Canada, as well as by the federal government.

ROTATE Q0 and Q0

9. There are a number of different things that information privacy legislation, whether federal or provincial, could provide or do, and I'd like to know how important it would be to you personally for the legislation to include each of the following requirements. Please use a 7 point scale, where 1 means it is not at all important and 7 means it is very important. The first one is (READ ITEM - RANDOMIZE). What about (READ NEXT ITEM)?

   - obtain individuals' permission to collect information about them
   - obtain individuals' permission to use information internally, such as for sales, marketing, or research

- provide access to individuals to information about themselves and allow them to correct errors
- obtain individuals' permission to share information with outside organizations
- ensure that all internet transactions are protected
- inform consumers how they use information about them
- be accountable to an independent authority

10. There are some specific kinds of information about people that could be covered by information privacy legislation, and I'd like to know how important it is to you personally for legislation to cover each of the following kinds of information. Please use a 7 point scale, where 1 means it is not at all important and 7 means it is very important. The first one is (READ ITEM - RANDOMIZE). What about (READ NEXT ITEM)?

    - Employee information; that is, personal information collected by employers
    - Consumer information; that is, personal information collected by businesses and organizations about their customers or members
    - Patient information; that is, personal information collected by doctors or other kinds of health care providers and businesses
    - Financial information
    - Internet usage information

11. Now, there are different ways that information privacy legislation might be applied to businesses and organizations. Please tell me whether you agree or disagree with the following ideas about how legislation could be applied, this time using a 7 point scale where 1 means you strongly disagree with the idea and 7 means you strongly agree with it. (READ ITEM - RANDOMIZE)

    - Businesses and organizations across Canada should be subject to the same information privacy laws, not different laws from province to province.
    - Private sector businesses and organizations should be subject to the same information privacy laws as government and government agencies.
    - All types of private sector businesses and organizations should be subject to the same information privacy laws, regardless of their size or the nature of their business.

12. I am now going to read you some statements that other people have made about this issue, and I'd like to know whether you agree or disagree with each one. Please use that same 7 point scale, where 1 means you strongly disagree and 7 means you strongly agree with what these people have said. (READ ITEM - RANDOMIZE).

    - With the internet and other new technology, it's impossible to be completely certain that personal information is kept completely private.
    - The internet has made it more important than ever that information privacy be protected.
    - Privacy legislation will just create more red tape for businesses, and that's bad for the economy.
    - Privacy legislation will help businesses in the long run, because consumers will trust them more.
    - It's more important to protect consumers than to make things easier for businesses.

13. And finally, thinking about everything that we've discussed today about information privacy, please tell me how concerned are you personally about the issue of information privacy. Please use a scale from 1 to 7 where 1 means you are not at all concerned and 7 means you are very concerned.

DEMOGRAPHIC SECTION

And, before I let you go, I just need to ask you a few questions for our statistical calculations.

14. In what year were you born?

15. What is the highest level of formal education that you have completed?

- Grade school or some high school
- Complete high school
- Technical, vocational post-secondary
- Some university
- Complete university degree
- Post graduate degree

16. Do you have regular access to the internet, either at home or at work or both? (PROBE)

- Yes, at home
- Yes, at work
- Yes, both
- No access at all
- Don't know

17. Do you have children under the age of 19 living with you on a regular basis?

- Yes
- No
- Don't know

18. And, finally, which of the following categories best describes your family income? That is, the combined total income before taxes of all persons in your household?

- Under $10,000
- $10,000 to $19,999
- $20,000 to $29,999
- $30,000 to $39,999
- $40,000 to $49,999
- $50,000 to $59,999
- $60,000 to $69,999
- $70,000 to $79,999
- $80,000 to $99,999
- $100,000 and over

Thank You For You Co-Operation!

APPENDIX III – WITNESS LIST

	Public Hearing	Submission Number
Archives Association of British Columbia		IPPS-sub-33
BC Civil Liberties Association	20-Jan-00 Vancouver	IPPS-sub-14
BC Freedom of Information and Privacy Association	20-Jan-00 Vancouver	IPPS-sub-12
BC Freedom of Information and Privacy Association and the BC Coalition of People with Disabilities	20-Jan-00 Vancouver	IPPS-sub-11
Bell Canada		IPPS-sub-25
Canada Trust		IPPS-sub-21
Canadian Association of Financial Institutions in Insurance		IPPS-sub-1
Canadian Bankers Association		IPPS-sub-9
Canadian Bar Association, BC Branch	20-Jan-00 Vancouver	IPPS-sub-15
Canadian Marketing Association		IPPS-sub-28
Canadian Institute for Health Information		IPPS-sub-32
Canadian Life and Health Insurance Association, Inc.	20-Jan-00 Vancouver	IPPS-sub-6
Equifax Canada Inc.	24-Jan-00 Victoria	IPPS-sub-17
Health Employers Association of British Columbia		IPPS-sub-30
Insurance Bureau of Canada	20-Jan-00 Vancouver	IPPS-sub-10
IMS Health Canada		IPPS-sub-26
Information, Science & Technology Agency		IPPS-sub-34
Professional Marketing Research Society of Canada	20-Jan-00 Vancouver	IPPS-sub-13
Retail Council of Canada	21-Jan-00 Richmond	IPPS-sub-16
Colin Bennett		IPPS-sub-27
Thomas Bryant		IPPS-sub-3
Brian Calder		IPPS-sub-20
Anna-Lise Cooke		IPPS-sub-4
Joseph Edwards	21-Jan-00 Richmond	IPPS-sub-19
Sheila Haegedorn	24-Jan-00 Victoria	IPPS-sub-18
Cheryl Leite		IPPS-sub-29

Kelly Manning		IPPS-sub-24
David McKenzie		IPPS-sub-31
Peter Minten		IPPS-sub-8
Dorothy Olson		IPPS-sub-23
Suzanne Purcell		IPPS-sub-2
Marcell Stoer		IPPS-sub-7
Glenn Vaughan		IPPS-sub-22
Tim Walwyn		IPPS-sub-5

APPENDIX IV – REFERENCES

[1] Terms of Reference.

[2] Legislative Assembly of British Columbia. Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act.* July 1999. 43.

[3] Legislative Assembly of British Columbia. 41-43.

[4] Rick Kasper. Hansard Transcripts (January 20, 2000). Special Committee on Information Privacy in the Private Sector. 25.

[5] Canada. *Personal Information Protection and Electronic Documents Act.* Section 30.

[6] Kevin McKee. Hansard Transcripts (June 26, 2000) 126; and Chris Norman. Hansard Transcripts (July 4, 2000) 139.

[7] Canada. *Personal Information Protection and Electronic Documents Act.* Summary.

[8] Canada. *Personal Information Protection and Electronic Documents Act.* Sections 26(2)(b) and 30.

[9] "The federal government has already designated the Quebec act as substantially similar" to the *Personal Information Protection and Electronic Documents Act.* Recommendations of the Information, Science and Technology Agency to the Special Committee on Information Privacy in the Private Sector. November 2000. 2.

[10] Industry Canada. "Consumer Connection." Vol. 4 No. 1. (March 1999). < http://strategis.gc.ca >.

[11] Date of coming into force.

[12] Electronic Commerce Branch, Industry Canada. "Canadian Internet Commerce Statistics Summary Sheet." March 2, 2001.

[13] Electronic Commerce Branch, Industry Canada. 1. Boston Consulting Group (Canada). *Fast Forward 2.0. Taking Canada to the Next Level: Report of the Canadian E-Business Opportunities Roundtable.* February 2001. <http://e-com.ic.gc.ca/english/documents/ff2.pdf >; and Electronic Commerce Branch, Industry Canada. "Canadian Internet Commerce Statistics Summary Sheet." March 2, 2001. 1. < http://e-com.ic.gc.ca/using/en/e-comstats.pdf >.

[14] Electronic Commerce Branch, Industry Canada. "Review of Statistics Canada Survey Use of Information and Communication Technologies and Electronic Commerce." 2. <http://e-com.ic.gc.ca/english/documents/statsrev.pdf>.

[15] Bruce Phillips. "Submission of the Office of the Privacy Commissioner of Canada to the Standing Committee on Industry." December 2, 1998. < http://www.privcom.gc.ca/speech/archive/ >.

[16] KPMG. *KPMG 1998 Electronic Commerce Survey.* 3. < http://www.kpmg.co.nz/eb/showPub.cfm?id=81 >.

[17] David Flaherty. Special Committee to Review the *Freedom of Information and Protection of Privacy Act.* Hansard Transcripts (February 24, 1998). Mr. Flaherty also told that Committee: "An additional one that I only became aware of recently is our 350 independent schools in this province, 300 of which receive significant amounts of provincial funding, including Catholic schools and other independent schools. None of them is covered by the privacy provisions of our legislation. It's hard to argue, as a parent or a student in an independent school, that you shouldn't have basic privacy rights such as we have vis-à-vis the Saanich school board, for example."

[18] The Okanagan Knowledge Economy Project explains that "the knowledge society" (another term for the information society) is "predicated on the increased recognition of the important role the acquisition, creation, assimilation, dissemination and use of knowledge play in the economy." < http://www.marketropolis.com/okep/knowleco1.html >.

[19] National Science Board. *Science & Engineering Indicators - 1998.* Arlington, Virginia: National Science Foundation, 1998 (NSB 98-1). 8.5 - 8.6. < http://www.nsf.gov/sbe/srs/seind98/start.htm >.

[20] Measurements of the uptake of information technologies (IT) in all of these sectors are relative comparisons. When comparing IT use globally, it is clear that not all nations of the world have been able to access IT at the same levels as

most Western nations, and not all individuals, even in industrialized countries, can afford to access IT. The discrepancies in IT access are well recognized in the literature, and are commonly referred to as the "digital divide".

[21] KPMG 1998 Electronic Commerce Survey. 2.

[22] Ann Cavoukian. "Data Mining: Staking a Claim on Your Privacy." Information and Privacy Commissioner of Ontario. January 1998. 2

[23] Ann Cavoukian and Don Tapscott. Who Knows: Safeguarding Your Privacy in a Networked World. Toronto: Random House of Canada, 1995. 84-85.

[24] Reg Whitaker. *The End of Privacy: How Total Surveillance is Becoming a Reality.* New York: New Press, 1999. 126.

[25] Internet profiling came under public scrutiny last year when the banner advertiser DoubleClick purchased an offline consumer database. DoubleClick had planned to correlate its online profiles with this database of consumer information. Because marketing databases often include identifying information, this could have allowed DoubleClick to link the personal preferences gathered online with the names, addresses and phone numbers in the offline consumer database, and thereby uniquely identify individuals and their preferences. Doubleclick has had to suspend its plans to link its online and offline databases in response to public pressures. (Sandeep Junnarkar. "Double Click accused of unlawful consumer data use." CNET News.com. January 28, 2000. <http://news.cnet.com/news/0-1005-200-1534533.html>.

[26] Cavoukian. "Data Mining." 6.

[27] "Data Mining: An IBM Overview." < http://www.cs.bham.ac.uk/~anp/dm_docs/ibm_kdd_overview.html >; Pilot Software. "An Introduction of Data Mining: Discovering Hidden Value in your Data Warehouse." <http://www3.shore.net/~kht/text/dmwhite/dmwhite.htm >.

[28] Ann Cavoukian. "Data Mining: Staking a Claim on Your Privacy." Information and Privacy Commissioner of Ontario. January 1998. 16.

[29] Cavoukian. "Data Mining." 8-10.

[30] Michael Moynihan, in Mark Costello et al. "The Searchable Soul: Privacy in the Age of Information Technology." *Harpers Magazine.* January 2000: 57-68. 65.

[31] Max Kilger. "The Digital Individual." *The Information Society.* Vol. 10 (1994): 93-99. 97; and Reg Whitaker. *The End of Privacy: How Total Surveillance is Becoming a Reality.* New York: New Press, 1999. 123-138.

[32] Hansard Transcripts (January 20, 2000) 38.

[33] Ipsos-Reid. "BC Public and Business Attitudes to Information Privacy. Report submitted to the Special Committee on Information Privacy in the Private Sector." February 15, 2001. 33.

[34] Ipsos-Reid 38.

[35] Ipsos-Reid 30-32.

[36] Ipsos-Reid 43.

[37] Ipsos-Reid 41-42.

[38] Ipsos-Reid 39.

[39] Ipsos-Reid 38-39.

[40] Ipsos-Reid 39-40

[41] Ipsos-Reid 29.

[42] Ipsos-Reid 39-40.

[43] Ipsos-Reid 34.

[44] Submissions.

[45] Submissions.

[46] Submissions.

[47] Submissions.

[48] Ipsos-Reid 35.

[49] Ipsos-Reid 11.

[50] Ipsos-Reid 46.

[51] Ipsos-Reid 48.

[52] Ipsos-Reid 47-48.

[53] Ipsos-Reid 19.

[54] Ipsos-Reid 23.

[55] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 146.

[56] Ipsos-Reid 22.

[57] Ipsos-Reid 22.

[58] Ipsos-Reid 73.

[59] Submissions. Anna-Lise Cooke.

[60] Ipsos-Reid 22.

[61] Ipsos-Reid 47.

[62] Ipsos-Reid 21-22.

[63] Ipsos-Reid 23.

[64] Ipsos-Reid 22.

[65] Ipsos-Reid 48.

[66] Ipsos-Reid 51.

[67] Submissions. Suzanne Purcell.

[68] Ipsos-Reid 52.

[69] Ipsos-Reid 40-41.

[70] Ipsos-Reid 41.

[71] Ipsos-Reid Detailed Tables.

[72] Ipsos-Reid 40-41.

[73] Submissions. BC Civil Liberties Association.

[74] Hansard Transcripts (September 21, 2000). 155.

[75] Ipsos-Reid 23.

[76] Janlori Goldman and Zoe Hudson. "Exposed: A Health Privacy Primer for Consumers." Washington, D.C.: Health Privacy Project. Institute for Health Care Research and Policy. Georgetown University: December 1999. 2.

[77] Freedom of Information and Privacy Association. "Personal Health Information and the Right to Privacy: An Overview of Statutory, Common Law, Voluntary, and Constitutional Privacy Protections." Prepared for the BC Freedom of Information and Privacy Association by the BC Public Interest Advocacy Centre. Vancouver: March 2000.

[78] Michel Leger. "A Vital Link to the Future: The Canada Health Infoway." *Canadian Government Executive*. Vol. 6 No. 3 (May 2000): 20-22. 21

[79] Michel Leger 21.

[80] British Columbia Ministry of Health. "Telehealth in British Columbia: A Vision for the 21st Century." August 1999. < http://www.moh.hnet.bc.ca/him/moh/img/paper.html >

[81] Information Management Group. British Columbia Ministry of Health and Ministry Responsible for Seniors. *Information Resource Management Plan, 1998-2003.* January 30, 1998. 10. <http://www.hlth.gov.bc.ca/him/moh/irmp/chap3.html >.

[82] Sara Baase. *A Gift of Fire: Social, Legal and Ethical Issues in Computing.* New Jersey: Prentice Hall, 1997. 21.

[83] Jochen Moehr. Hansard Transcripts (September 21, 2000) 156.

[84] Ipsos Reid 53

[85] Submissions. IMS Health Canada.

[86] Hansard Transcripts. (September 21, 2000). 161.

[87] Richard Rosenberg. Hansard Transcripts. (September 21, 2000). 148.

[88] Ipsos-Reid 37-38.

[89] Jochen Moehr. Hansard Transcripts (September 21, 2000) 161.

[90] Jochen Moehr. Hansard Transcripts (September 21, 2000) 16.

[91] Sheila Haegedorn. Hansard Transcripts (January 24, 2000) 73.

[92] Industry Canada. "Consumer Connection." Vol. 4 No. 1. March 1999. http://strategis.gc.ca

[93] Alan Westin, qtd. in Denis C. Kratchanov. "Personal Information and the Protection of Privacy." Appendix M to *Proceedings of the 1995 meeting of the Uniform Law Conference of Canada.* Uniform Law Conference of Canada. Quebec City, PQ. August 1995. <http://www.law.ualberta.ca/alri/ulc/95pro/95e.htm>. Denis C. Kratchanov reports that this definition of the right to privacy that has been widely used, and has been accepted by both the Supreme Court of Canada and the United States Supreme Court.

[94] BC Civil Liberties Association and the BC Freedom of Information and Privacy Association. *The Privacy Handbook.* Vancouver, 1994. xix.

[95] William W. Black. *BC Human Rights Review: Report on Human Rights in British Columbia.* Government of British Columbia. December 1994. < http://www.bchrc.gov.bc.ca/home.htm >.

[96] John Godfrey, qtd. in *Privacy: Where Do We Draw the Line? Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities.* Canada: Standing Committee on Human Rights and the Status of Persons with Disabilities, April 1997. 5.

[97] BC Human Rights Commission. "Human Rights for the Next Millennium: BC Human Rights Code Amendments Recommended by the BC Human Rights Commission." January 19, 1998. <http://www.bchrc.gov.bc.ca/home.htm>.

[98] Ann Cavoukian, "Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation." Information and Privacy Commissioner of Ontario. September 1999. iv. <http://www.ipc.on.ca/english/pubpres/sum_pap/summary.htm >.

[99] Office of Consumer Affairs, Industry Canada.

[100] Office of Consumer Affairs, Industry Canada. "New Approaches to Consumer Law in Canada." October 1996. < http://strategis.ic.gc.ca/SSG/ca00318e.html >.

[101] Cavoukian "Privacy" 10.

[102] Cavoukian "Privacy" 19-20.

[103] For example, see David Loukidelis, Hansard (November 18, 1999) 20-21; and Cavoukian "Privacy" 26-29.

[104] Exceptions are generally made for publicly available information, and for matters concerning national security and defence, and crime detection and enforcement of criminal law.

[105] European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Article 25.

[106] Industry Canada. "Privacy: The Protection of Personal Information. Building Canada's Information Economy and Society." 1998. < http://e-com.ic.gc.ca/english/privacy/632d2.html >.

[107] Canadian Standards Association. *Plus 8300: Making the CSA Privacy Code Work for You: A Workbook on Applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to Your Organization.* 9.

[108] External Liaison Committee, Canadian Information Processing Society. "Privacy & Information Technology Paper - Implementation & Operational Guidelines." August, 1997. < http://www.cips.ca/it/position/privacy/#4 >.

[109] Canadian Legal Education Society of British Columbia. "Working with the Privacy Rules." 7. < http://www.cle.bc.ca/cle/analysis/articles/00-5020400-privacy.htm >.

[110] Canadian Standards Association 11.

[111] Canadian Standards Association 11.

[112] Canadian Legal Education Society of British Columbia 8.

[113] Canadian Legal Education Society of British Columbia 8.

[114] Canadian Standards Association 12.

[115] Submissions. BC Freedom of Information and Privacy Association.

[116] Canadian Standards Association 13.

[117] Canadian Standards Association 13-14.

[118] Canadian Standards Association 14.

[119] Canadian Standards Association 14.

[120] Canadian Standards Association 14.

[121] Canadian Standards Association 15.

[122] Canadian Standards Association 15.

[123] Canadian Standards Association 17.

[124] Canadian Standards Association 17.

[125] Canadian Standards Association 18.

[126] Canadian Standards Association 19.

[127] Canadian Standards Association 19.

[128] Submissions. Thomas Bryant.

[129] Ipsos-Reid. Detailed Tables. P. 70.

[130] Submissions. Professional Marketing Research Society.

[131] Submissions. Insurance Bureau of Canada.

[132] Submissions. Retail Council of Canada; Bell Canada.

[133] Ipsos-Reid 66.

[134] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 153.

[135] Canadian Bar Association, BC Branch.

[136] Ipsos-Reid 63.

[137] Ipsos-Reid 42.

[138] Ipsos-Reid 63.

[139] Submissions. Colin Bennett.

[140] Submissions. Canadian Association of Financial Institutions in Insurance.

[141] Ipsos-Reid 25.

[142] Ipsos-Reid 53.

[143] Submissions. Kelly Manning.

[144] Submissions. Richard Rosenberg.

[145] Colin H. H. McNairn and Alexander K. Scott. *A Guide to the Personal Information Protection and Electronic Documents Act.* Toronto and Vancouver: Butterworths, 2000. 9-10.

[146] Canadian Bar Association, BC Branch.

[147] Submissions. Canadian Association of Financial Institutions in Insurance.

[148] Submissions. Insurance Bureau of Canada.

[149] Ipsos-Reid 60.

[150] ISTA 7.

[151] ISTA 7.

[152] Submissions. BC Civil Liberties Association.

[153] Ipsos-Reid 15.

[154] Submissions. BC Freedom of Information and Privacy Association and BC Coalition of People with Disabilities.

[155] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 145.

[156] Submissions. BC Freedom of Information and Privacy Association and BC Coalition of People with Disabilities.

[157] Submissions. BC Civil Liberties Association.

[158] Submissions. Canadian Bar Association, BC Branch.

[159] Submissions. BC Civil Liberties Association.

[160] Submissions. Canadian Association of Financial Institutions in Insurance.

[161] Submissions. Canada Trust.

[162] Ipsos-Reid 59.

[163] McNairn and Scott 16.

[164] McNairn and Scott 16-17.

[165] Ipsos-Reid 52.

[166] ISTA 5.

[167] Ipsos-Reid 59.

[168] Submissions. Colin Bennett.

[169] Jochen Moehr. Hansard Transcripts (September 21, 2000) 160.

[170] Submissions. BC Freedom of Information and Privacy Association and BC Coalition of People with Disabilities. Rosenberg.

[171] Submissions. Canadian Institute for Health Information.

[172] The Alberta *Health Information Act* received Royal Assent in 1999 but has not yet been proclaimed.

[173] Submissions. Colin Bennett.

[174] David Loukidelis. Hansard Transcripts (September 21, 2000) 155.

[175] Hansard Transcripts (September 21, 2000) 155.

[176] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 150.

[177] Submissions. IMS Health Canada.

[178] Submissions. IMS Health Canada.

[179] Ann Cavoukian. Information and Privacy Commissioner of Ontario. "Submission to the Ministry of Health and Long-Term Care in Response to Ontario's Proposed Personal Health Information Privacy Legislation for the Health Sector (Health Sector Privacy Rules)." October 2000. 11.

[180] Freedom of Information and Privacy Association 8.

[181] David Loukidelis. Hansard Transcripts (September 21, 2000) 162.

[182] Freedom of Information and Privacy Association 9.

[183] McInerney v. MacDonald, [1992] 2 S.C.R. 138 at 148, qtd. in Freedom of Information and Privacy Association 8.

[184] Submissions. IMS Health Canada.

[185] Submissions. IMS Health Canada.

[186] Submissions. IMS Health Canada.

[187] Canadian Medical Association. "Health Information Privacy Code." August 15, 1998. 10.

[188] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 158.

[189] Ipsos-Reid 53.

[190] Submissions.

[191] Richard Rosenberg. Hansard Transcripts (September 21, 2000) 149.

[192] Submissions. Colin Bennett.

[193] 20.
[194] Submissions. Canadian Marketing Association.

[195] 7-8.
[196] Submissions.

[197] Submissions. Archives Association of British Columbia.

[198] Submissions. Equifax Canada.

[199] Submissions. Colin Bennett.

[200] David Flaherty. Hansard Transcript (February 24, 1998).

[201] Canada. *Personal Information Protection and Electronic Documents Act.*

[202] 11.

[203] 12.

[204] Submissions. Professional Marketing Research Society.

[205] Ipsos-Reid 25.

[206] Submissions. Colin Bennett.

[207] Ipsos-Reid 25.

[208] Submissions. Colin Bennett.

[209] Ipsos-Reid 60.

[210] Ipsos-Reid 35-36.

[211] Ipsos-Reid 32-33.

[212] Ipsos-Reid 35.

[213] Ipsos-Reid 26.

[214] Industry Canada. Strategis. "Electronic Commerce in Canada: Backgrounder". 2000-12-10. < http://e.com.ic.ca/english/fastfacts/43d9.html >.

[215] Terms of Reference.

[216] Byron Barnard. Hansard (June 12, 2000) 112.

[217] Bill 32-2000 *Electronic Transactions Act*. Section 9(c). < http://www.legis.gov.bc.ca/2000/1st_read/gov32-1.htm >.

[218] Information, Science and Technology Agency. "Backgrounder: Electronic Transactions Act (ETA)". < http://www.ista.gov.bc.ca/News/2000/00_53nr_bg.htm >.

[219] Information, Science and Technology Agency. Backgrounder.

[220] Byron Barnard. Hansard Transcripts (June 12, 2000) 111-112.

[221] Information, Science and Technology Agency. Backgrounder.

[222] Industry Canada. "Speaking Notes for the Honourable John Manley, Ministry of Industry. Presentation to the National Press Club. Canada's Cryptography Policy." October 1, 1998. < http://e-com.ic.gc.ca/english/speeches/42d3.html >. Industry Canada. "Public Discussion Paper on Setting a Cryptography Policy Framework for Canada: Backgrounder." 2000-12-10. < http://e-com.ic.gc.ca/english/crypto/631d22.html >.

[223] Industry Canada. "Summary of Canada's Cryptography Policy: Backgrounder." 2000-12-10. <http://e-com.ic.gc.ca/english/fastfacts/43d7.html >

[224] J. Hamilton. Electronic Commerce Branch. Industry Canada. "Addressing the Trust Agenda: Electronic Authentication. Summary of the Consultation Process." February 2001. 4. < http://e-comm.ic.gc.ca/ >.

[225] J. Hamilton. 4.